الجريمة الالكترونية

وكيفية مواجهتها

Cybercrimes

Societies and How to Tackle Them

كتابة واعداد

أ. أريج عبد الرزاق بنيس

مقدمة

بسم الله الرحمن الرحيم

أتقدم بهذا العمل وقلبي يعتصره الحزن لغياب والدي الحبيب، رحمه الله وأسكنه فسيح جناته. كان والدي، وسيظل دائما، مصدر إلهامي ونبراسي في طلب العلم والمعرفة.

وإنني، وأنا أخط هذه الكلمات، أستحضر ذكراه العطرة وتوجيهاته الحكيمة التي ما زالت تنير دربي.

أقدم هذا الكتاب إلى روحه الطاهرة، معبرا عن عميق احترامي وامتناني لكل ما قدمه لي من دعم وتشجيع. كما أتوجه بالشكر والدعاء لوالدتي الغالية، حفظها الله ورعاها، التي وقفت إلى جانبي في كل خطوة، وما زالت سندي وملاذي.

يتناول هذا الكتاب موضوع الجريمة الإلكترونية، وهو من القضايا الملحة في عصرنا الرقمي. وإنني آمل أن يكون هذا العمل امتداداً للقيم النبيلة التي غرسها والدي فيّ، وأن يسهم في خدمة المجتمع وحمايته من مخاطر هذه الظاهرة المتنامية.

وإنني، إذ أقدم هذا العمل، أسأل الله أن يجعله في ميزان حسنات والدي، وأن يجزيه خير الجزاء على ما قدمه لي ولاخوتي

الباب الأول
الفصل الأول
الجريمة الالكترونية
ماهيتها وأسبابها وطرق مكافحتها

أولا تعريف الجريمة الإلكترونية : الجريمة السيبرانية (بالإنجليزية Cybercrime(جريمة العصر)هي نوع حديث من الجرائم التي حيرت العالم في تصنيفها.

الجريمة الالكترونية: هي كل فعل يتعمد مرتكبه الإضرار بغيره عن طريق الشبكة المعلوماتية جريمة عابرة للقارات بمعنى أنها لا تعترف بالحدود الجغرافية للدول وعدم اشتراط تواجد الجاني في مكان الجريمة مثل السابق حيث كان هذا الشرط ركن من أركان الجريمة فقد يكون الجاني في مكان والمجني عليه في مكان أو بلد آخر.

ويمكن تعريف الجريمة الإلكترونية على أنها أي مخالفة ترتكب ضد أفراد أو جماعات بدافع جرمي ونية الإساءة لسمعة الضحية أو لجسدها أو عقليتها، سواء كان ذلك بطريقة مباشرة أو غير مباشرة، وأن يتم ذلك باستخدام وسائل الاتصالات الحديثة مثل الانترنت, غرفة الدردشة،البريد الإلكتروني.

الجرائم الإلكترونية جرائم صعبة الإثبات حيث انه من الصعب إثبات مرتكب هذه الجريمة وماهيته الشخصية وأي قانون يطبق.

الجريمة الإلكترونية ماهيتها :

1. تعتبر من الجرائم المعقدة وذلك لصعوبة معرفة مرتكبها إلا باستخدام وسائل أمنية ذات تقنية عالية.
2. صعوبة قياس الضرر المترتب عليها كونه ضررا يمس الكيانات المعنوية والقيم المادية أو كلاهما سوية.
3. سهولة الوقوع فيها بسبب غياب الرقابة الأمنية.
4. سهولة اخفاء وطمس معالم الجريمة وآثارها والدلائل التي تدل على مرتكبها.
5. سلوك غير أخلاقي واصبح منتشر بكافة دول العالم نتيجة غياب العقاب.
6. جريمة لا تتقيد بمكان أو زمان محددين.

نبذة تاريخية

- **المرحلة الأولى**

تمتد من شيوع استخدام الحاسب الآلي في الستينات إلى غاية 1970، اقتضت معالجة على المقالات تمثلت في التلاعب بالبيانات المخزنة وتدميرها

- **المرحلة الثانية**

في الثمانينات حيث طفح على السطوح مفهوم جديد لجرائم الكمبيوتر والإنترنت تمثلت في اقتحام الأنظمة ونشر الفيروسات

- **المرحلة الثالثة**

في التسعينات حيث شهدت هذه المرحلة تناميا هائلا في حقل الجرائم الإلكترونية، نظرا لانتشار الإنترنت في هذه الفترة مما سهل من عمليات دخول الأنظمة واقتحام شبكة المعلومات مثلا: تعطيل نظام تقني، نشر الفيروسات...الخ

مفاهيم الجريمة الإلكترونية

أدت الحداثة التي تتميز بها الجريمة الإلكترونية واختلاف النظم القانونية والثقافية بين الدول إلى اختلاف في مفهوم الجريمة الإلكترونية من بينها:

- حسب اللجنة الأوروبية فإن مصطلح الجريمة الإلكترونية يضم كل المظاهر التقليدية للجريمة مثل الغش وتزييف المعلومات، ونشر مواد إلكترونية ذات محتوى مخل بالأخلاق أو دعوى لفتن طائفية.
- حسب وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة عبر الإنترنت بأنها «أي جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها».
- حسب منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الإنترنت «هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات ونقلها».

بعض تسميات الجرائم الإلكترونية

- جرائم الإنترنت (Computer crime)
- جرائم التقنية العالية (Hi-tech crime)
- الجريمة السيبرانية (Cybercrime)

خصائص وسمات الجرائم الإلكترونية

- سهولة ارتكاب الجريمة بعيدا عن الرقابة الأمنية، فهي ترتكب عبر جهاز الكمبيوتر مما يسهل تنفيذها من قبل المجرم دون أن يراه أحد أو يكتشف.
- صعوبة التحكم في تحديد حجم الضرر الناجم عنه قياسا بالجرائم العادية فالجرائم الإلكترونية تتنوع بتنوع مرتكبيها وأهدافهم وبالتالي لا يمكن تحديد حجم الأضرار الناجمة عنها.
- مرتكبيها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم أمراً صعباً أعمارهم تتراوح غالبا ما بين (18 إلى 48 سنة).
- تنطوي على سلوكيات غير مألوفة عن المجتمع.
- اعتبارها أقل عنفاً في التنفيذ فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية، لأن المجرم عند تنفيذه لمثل هذه الجرائم لا يبذل جهدا فهي تطبق على الأجهزة الإلكترونية وبعيدا عن أي رقابة مما يسهل القيام بها.
- جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه، بالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكابها عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.
- سهولة إتلاف الأدلة من قبل الجناة، في المعلومات المتداولة عبر الإنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة وهي عبارة عن نبضات إلكترونية غير مرئية مما يجعل طمس ومحو الدليل أمر سهل.

الجرائم الإلكترونية لها تأثيرات سلبية كبيرة على الأفراد والمؤسسات والدول تشمل هذه التأثيرات الخسائر المالية، انتهاك الخصوصية، وتعطيل الخدمات الحيوية, لذلك من الضروري تطوير استراتيجيات فعالة لمكافحة هذه الجرائم وحماية الأنظمة الرقمية من الاختراقات

الفصل الثاني

المجرم الإلكتروني

المجرم الإلكتروني هو شخص يستخدم التكنولوجيا الرقمية والإنترنت لارتكاب جرائم مختلفة. يتميز بقدرته على تحويل لغته إلى لغة رقمية باستخدام الحاسوب وأدوات الاتصال الرقمية لتنفيذ أفعاله الإجرامية.

يختلف المجرم الإلكتروني عن المجرم التقليدي بسماته الخاصة، حيث يتميز بمهارات تقنية عالية ودوافع متنوعة قد تشمل الكسب المادي أو الدوافع السياسية أو حتى التسلية.

سمات المجرم الإلكتروني

يمكن تحديد عدة سمات رئيسية للمجرم الإلكتروني:

المهارات التقنية العالية: غالباً ما يتمتع المجرمون الإلكترونيون بمعرفة متقدمة في مجال تكنولوجيا المعلومات والبرمجة

العمل عن بعد: يمكنهم تنفيذ جرائمهم من أي مكان في العالم دون الحاجة للتواجد في موقع الجريمة

السرعة في التنفيذ: قدرتهم على ارتكاب الجرائم بسرعة كبيرة، أحياناً بمجرد ضغطة زر

التخفي وصعوبة التتبع: يستخدمون تقنيات متطورة لإخفاء هوياتهم وتجنب الكشف عنهم

التنوع في الدوافع: قد تكون دوافعهم مادية أو سياسية أو حتى لمجرد التسلية

الاستغلال الداخلي: نسبة كبيرة من المجرمين الإلكترونيين هم موظفون داخليون في المؤسسات المستهدفة، مثل محللي البيانات والمبرمجين

القدرة على التكيف: يتميزون بسرعة التأقلم مع التطورات التكنولوجية واستغلالها في أنشطتهم الإجرامية

العمل بشكل فردي أو ضمن مجموعات منظمة: يمكنهم العمل منفردين أو ضمن شبكات إجرامية معقدة

الذكاء والإبداع: غالباً ما يتمتعون بمستوى عالٍ من الذكاء والقدرة على ابتكار أساليب جديدة للاحتيال والاختراق

عدم استخدام العنف الجسدي: يميلون إلى ارتكاب "جرائم ناعمة" لا تتطلب استخدام القوة البدنية

هذه السمات تجعل من المجرمين الإلكترونيين تهديداً فريداً يتطلب أساليب مكافحة متخصصة ومتطورة

كيف يمكن تحديد المجرم الإلكتروني

يمكن تحديد المجرم الإلكتروني من خلال عدة طرق وتقنيات، منها:

1. **تحليل السجلات والأحداث الأمنية:** مراقبة وتحليل سجلات الأنظمة والشبكات للكشف عن أي نشاط مشبوه أو غير طبيعي, هذا يساعد في اكتشاف محاولات الاختراق مبكراً.
2. **فحص ملفات البرمجيات الخبيثة وعناوين IP:** استخدام أدوات متخصصة لفحص الملفات المشبوهة وتحليل عناوين IP المرتبطة بالهجمات.
3. **تحليل الاتصالات الشبكية:** مراقبة وتحليل حركة البيانات على الشبكة باستخدام أدوات مثل Wireshark للكشف عن أنماط الاتصال المشبوهة.
4. **التحليل الجنائي الرقمي:** استخدام تقنيات متقدمة لاستخراج وتحليل البيانات من الأجهزة الرقمية للحصول على أدلة.
5. **تتبع البصمات الرقمية:** إنشاء ملف تعريف فريد للمجرم الإلكتروني يساعد في تتبع نشاطاته عبر الإنترنت.
6. **التعاون مع جهات إنفاذ القانون:** الإبلاغ عن الجرائم الإلكترونية للسلطات المختصة مثل مكتب التحقيقات الفيدرالي (FBI) للمساعدة في التحقيق.
7. **تعزيز الوعي الأمني:** تدريب الموظفين على التعرف على علامات الاختراق والتهديدات الأمنية وكيفية الإبلاغ عنها.

8. **استخدام أنظمة كشف ومنع الاختراق:** تثبيت وتحديث برامج الأمان مثل جدران الحماية وأنظمة كشف التسلل لتحديد ومنع الهجمات.
9. **تحليل أنظمة التشغيل:** فحص أنظمة التشغيل للكشف عن أي تغييرات غير مصرح بها أو برامج ضارة مثبتة.
10. **مراقبة الأنشطة المشبوهة:** الانتباه إلى أي سلوك غير عادي على الشبكة أو الأنظمة، مثل محاولات تسجيل الدخول المتكررة أو نقل كميات كبيرة من البيانات.

من المهم اتباع نهج شامل ومتعدد الطبقات في الأمن السيبراني للتمكن من تحديد المجرمين الإلكترونيين بفعالية والتصدي لهجماتهم.

تقنيات تحديد موقع المجرم الإلكتروني

يمكن للشرطة تحديد موقع المجرم الإلكتروني من خلال عدة تقنيات وأساليب متطورة، منها:

1. **تحليل البيانات الجغرافية:** يمكن تحديد موقع الجهاز المستخدم في الجريمة والاحتفاظ بالبيانات الجغرافية المرتبطة به, هذه المعلومات قد تساعد في تحديد الموقع الفعلي للمجرم.
2. **استخراج البيانات من الأجهزة:** يمكن استخدام أدوات الأدلة الجنائية المتخصصة لاستخراج البيانات من صور الذاكرة وتحليله, هذا قد يكشف عن معلومات مهمة حول موقع المجرم وأنشطته.
3. **تحليل بيانات الناقل والجهاز:** يمكن استخدام هذه البيانات لتأكيد المعلومات من مصادر أخرى، مثل لقطات فيديو المراقبة أو شهادات الشهود، مما قد يساعد في تحديد موقع المجرم.
4. **استخدام أدوات متخصصة:** تقوم الشرطة باستخدام أدوات تحقيق متطورة في الأدلة الجنائية للأجهزة المحمولة، والتي تمكنهم من الوصول إلى ذاكرة الجهاز وتجاوز أنظمة الحماية.

5. **تتبع الاتصالات الشبكية:** مراقبة وتحليل حركة البيانات على الشبكة قد يساعد في تحديد مصدر الهجمات الإلكترونية.
6. **التعاون مع مزودي خدمة الإنترنت:** يمكن للشرطة العمل مع مزودي الخدمة للحصول على معلومات حول عناوين IP المستخدمة في الجريمة.
7. **استخدام تقنيات التتبع المتقدمة:** هناك تقنيات حديثة يمكنها تحديد موقع الأشخاص المطلوبين بدقة عالية.
8. **الاستعانة بوحدات متخصصة:** تعمل وحدات مكافحة الجرائم الإلكترونية على دراسة القضايا وتتبع المجرمين باستخدام تقنيات متطورة.

من المهم الإشارة إلى أن عملية تحديد موقع المجرم الإلكتروني قد تكون معقدة وتتطلب جهوداً متضافرة من قبل فرق متخصصة في الأمن السيبراني والتحقيقات الجنائية الرقمية.

التحديات التي تواجه الشرطة في تحديد موقع المجرم الإلكتروني

هناك عدة تحديات رئيسية تواجه الشرطة في تحديد موقع المجرم الإلكتروني:

1. **فقدان البيانات:** بسبب التشريعات مثل GDPR، قد يتم حرمان الشرطة من الوصول إلى البيانات الضرورية للتحقيق. كما أن استخدام التشفير والعملات المشفرة يجعل من الصعب الحصول على أدلة مجرمة.
2. **فقدان الموقع:** استخدام تقنيات مثل الشبكة المظلمة والتخزين السحابي يجعل من الصعب تحديد الموقع الفعلي للمجرمين أو البنية التحتية الإجرامية.
3. **اختلاف الأطر القانونية:** تختلف القوانين بين الدول مما يعيق التحقيقات عبر الحدود وجمع الأدلة الإلكترونية.
4. **عوائق التعاون الدولي:** عدم وجود إطار قانوني موحد عالمياً يعيق التعاون الدولي الفعال، خاصة في الهجمات الكبيرة متعددة القارات.
5. **تحديات الشراكة بين القطاعين العام والخاص:** عدم وجود إطار قانوني واضح يحدد كيفية تعاون القطاع الخاص مع الشرطة دون انتهاك خصوصية العملاء.
6. **التقنيات الناشئة:** التطور السريع للتقنيات مثل الحوسبة الكمومية والذكاء الاصطناعي يخلق تحديات جديدة.

7. **نقص الموارد والخبرات:** العديد من أجهزة الشرطة المحلية تفتقر إلى الموارد والخبرات اللازمة للتعامل مع الجرائم الإلكترونية المعقدة.
8. **الطبيعة العابرة للحدود:** صعوبة التعامل مع الجرائم التي تتجاوز الحدود الوطنية والدولية.
9. **التحديات التقنية:** الحاجة إلى مهارات وأدوات متخصصة لتتبع المجرمين الذين يستخدمون تقنيات لإخفاء هويتهم وموقعهم.

لمواجهة هذه التحديات، يتطلب الأمر تعاوناً دولياً أكبر، وتحديث التشريعات، وتطوير القدرات التقنية، وتعزيز التعاون بين القطاعين العام والخاص.

توضيح الفقرة 1 :ما هو نظام GDPR : هو نظام يهدف إلى تعزيز حماية البيانات الشخصية وتوحيد قوانين حماية البيانات عبر الاتحاد الأوروبي، مما يؤثر على ممارسات الشركات العالمية في التعامل مع البيانات الشخصية.

وتوضيح للفقرة 2: وما المقصود بالشبكة المظلمة والتخزين السحابي :

الشبكة المظلمة أو الدارك نت : هي شبكة خاصة يتم الاتصال فيها فقط بين أطراف موثوقة عبر بروتوكولات ومنافذ غير قياسية. تتميز هذه الشبكة بما يلي

لا يمكن الوصول إليها عبر المتصفحات التقليدية أو فهرستها بواسطة محركات البحث العادية مثل جوجل.

تستخدم تقنيات تشفير متقدمة لإخفاء هوية المستخدمين وأنشطتهم

تحتوي على مجموعة متنوعة من المواقع والأسواق التي تجمع بين أفراد يشاركون في أنشطة غير مشروعة أو مشبوهة

يتم استخدامها للاتجار بالمعلومات المسروقة والبيانات الشخصية وغيرها من الأنشطة الإجرامية

يمكن استخدامها أيضاً لأغراض شرعية مثل الانضمام إلى مجتمعات خاصة أو شبكات اجتماعية غير معروفة

رغم أن الوصول إلى الشبكة المظلمة ليس غير قانوني بحد ذاته، إلا أنها تشكل تحدياً كبيراً للأجهزة الأمنية بسبب صعوبة تتبع الأنشطة الإجرامية فيها

التخزين السحابي : هو نموذج لتخزين البيانات والملفات عبر الإنترنت باستخدام خوادم افتراضية متعددة يديرها مزود خدمة سحابية. يتميز هذا النوع من التخزين بعدة مزايا رئيسية

الوصول السهل: يمكن الوصول إلى البيانات من أي مكان وفي أي وقت عبر الإنترنت

المرونة: يمكن زيادة أو تقليل مساحة التخزين بسهولة حسب الحاجة

الحماية والنسخ الاحتياطي: توفر معظم الخدمات حماية للبيانات ونسخ احتياطية تلقائية

فعالية التكلفة: الدفع مقابل الاستخدام الفعلي فقط، دون الحاجة لشراء أجهزة إضافية

سهولة المشاركة: تسهيل مشاركة الملفات والتعاون بين المستخدمين

تتوفر ثلاثة أنواع رئيسية للتخزين السحابي: مخزن الكائنات، مخزن الملفات، ومخزن الكتل. رغم مزاياه العديدة، يواجه التخزين السحابي بعض التحديات مثل الاعتمادية على اتصال الإنترنت وقضايا الأمان والخصوصية

مسميات مرتكبو الجرائم الإلكترونية

- **القراصنة الهواة Hackers**

يقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الالية وبعضهم يطلق عليهم صغار نوابغ المعلوماتية وأغلبهم من الطلبة. تضم هذه الطائفة الاشخاص الذين يستهدفون من الدخول إلى انظمة الحاسبات الالية غير المصرح لهم بالدخول إليها. كسر الحواجز الامنية الموضوعة لهذا الغرض وذلك بهدف الخبرة أو الفضول.

- **القراصنة المحترفين Crackers**

أعمارهم تتراوح ما بين 25–45 سنة في الغالب يكونون ذوي مكانة في المجتمع ودائماً ما يكونوا من المختصين في مجال التقنية الإلكترونية. هم أكثر خطورة وعادة مايعودون إلى ارتكاب الجريمة مرة أخرى.

- **طائفة الحاقدين**

يطلق عليهم المنتقمون لأنها تنطلق ضد أصحاب العمل والمنشآت التي كانوا يعملون بها وانتقاماً من رب العمل وهم أقل خطورة، يرى الباحثون أن أهداف وأغراض الجريمة

غير متوفرة لدى هذه الطائفة فهم لا يهدفون إلى إثبات قدراتهم التقنية ومهاراتهم الفنية ويبغون تحقيق مكاسب مادية أو سياسية، بل يعمدون إلى إخفاء وإنكار أفعالهم واغلب أنشطتهم تتم باستخدام تقنيات زراعة الفيروسات والبرامج الضارة تخريب الأنظمة المعلوماتية.

- **طائفة المتطرفين**

يعرف التطرف في هذا المجال بأنه عبارة عن انشطة توظف شبكة الإنترنت في نشر وبث واستقبال وإنشاء المواقع والخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري، مما دفع بعض المتشددين إلى سلوك الطريق الإجرامي وأصبح هناك ما يعرف بـ المجرم المعلوماتي المتطرف الذي يستعمل بما في ذلك للشبكات الإعلامية الإخبارية التي تتبع نشاطات الجماعية ونشر بيانات وتصريحات قادتها، وعادة ما يقوم هؤلاء بالاتصال من مقاهي ومكاتب الإنترنت يستعملون كافة المواقع الإلكترونية التي تسعى لتحقيق أغراض دعائية لصالحهم.

- **طائفة المتجسسين**

يقوم هؤلاء بالعبث أو الإتلاف محتويات الشبكة من جانب ومن جانب آخر وهو الأهم والذي يشكل الخطر الحقيقي على تلك المواقع على سبيل المثال قد يتم تنزيل الأسرار الصناعية من كمبيوتر في إحدى الشركات وإرسالها بالبريد الإلكتروني مباشرة إلى منافستها، ومن أهم أهداف هذه الطائفة في استخدام الأنظمة المعلوماتية هي الحصول على معلومات الأعداء والأصدقاء على حد سواء.

- **طائفة مخترقي الأنظمة:**

يتبادل أفراد هذه الطائفة المعلومات فيما بينهم بغية اطلاع بعضهم على مواطن الضعف في الانظمة المعلوماتية وتجري عملية التبادل للمعلومات بينهم بواسطة النشرات الاعلامية الإلكترونية مثل: مجموعات الأخبار، بل إن أفراد هذه الطائفة يتولون عقد المؤتمرات لكافة مخترقي الانظمة المعلوماتية بحيث يدعى إليها الخبراء من بينهم للتشاور حول وسائل الاختراق وآليات نجاحها.

خصائص وسمات مرتكبو الجرائم

- شخص ذو مهارات فنية عالية متخصص في الجرائم المعلوماتية يستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور والشفرات ويسبح في عالم الشبكات، ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسيب من خلال الشبكات.
- شخص قادر على استخدام خبراته في الاختراق وتغيير المعلومات.
- شخص قادر على تقليد البرامج أو تحويل اموال.
- شخص محترف في التعامل مع شبكات الحاسبة.
- شخص غير عنيف لأن تلك الجريمة لا تلجأ للعنف في ارتكابها.
- شخص يتمتع بذكاء إذ يمكنه التغلب على كثير من العقبات التي تواجهه أثناء ارتكابه الجريمة، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الانظمة الامنية حتى لا تستطيع ان تلاحقه وتتبع أعماله الاجرامية من خلال الشبكات أو داخل اجهزة الحواسب ,الإجرام المعلوماتي هو اجرام ذكاء.
- شخص اجتماعي له القدرة على التكيف مع الآخرين.

(هي نفس خصائص ومسميات المجرم الالكتروني)

دوافع ارتكاب الجريمة الإلكترونية

- **دوافع مادية** ويتمثل في:
- تحقيق الكسب المادي: تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الإنترنت. نظراً للربح الكبير، وغالباً ما يكون الدافع لارتكاب هذه الجريمة هو وقوع الجاني في مشاكل مادية مثال على ذلك تحويل حساب مالي إلى حسابه.

- **دوافع شخصية** وتتمثل في:
  - **الرغبة في التعلم** يكرس مرتكبو هذه الجريمة وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية.
  - **دوافع ذهنية أو نمطية**: غالباً ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في إثبات الذات وتحقيق الانتصار على تقنية الانظمة المعلوماتية دون أن يكون لهم نوايا آثمة.
  - **دافع الانتقام:** تعد من أخطر الدوافع التي يمكن أن تدفع شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته.
  - **دافع التسلية** هي جريمة ترتكب من اجل التسلية لايقصد من ورائها احداث جرائم.
  - **دافع سياسي** يتم غالباً في المواقع السياسية المعادية للحكومة، ويتمثل في تلفيق الأخبار والمعلومات ولو زوراً أو حتى الاستناد إلى جزء بسيط جداً من الحقيقة ومن ثم نسخ الأخبار الملفقة حولها، تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم.

باتباع هذه الفئات والدوافع، يمكن فهم طبيعة المجرم الإلكتروني بشكل أفضل وتطوير استراتيجيات أكثر فعالية لمكافحة الجرائم الإلكترونية

الفصل الثالث

أهداف الجرائم الإلكترونية

أهداف الجرائم الإلكترونية تشمل:

- الحصول على معلومات سرية: مثل بيانات البنوك والمؤسسات والحكومات والأفراد، واستخدامها للابتزاز أو تحقيق مكاسب مادية أو سياسية.
- الكسب المادي أو المعنوي: من خلال سرقة الأموال أو المعلومات لتحقيق مكاسب غير مشروعة.
- تشويه السمعة والابتزاز: تهديد الضحايا بنشر معلوماتهم الخاصة لإجبارهم على دفع المال أو تنفيذ مطالب معينة.
- أهداف سياسية: مهاجمة مواقع حكومية أو نشر أخبار كاذبة لتحقيق أهداف سياسية معينة.

أدوات الجريمة الإلكترونية

يمكن تلخيص أدوات الجريمة الإلكترونية كما يلي:

- البرمجيات الخبيثة: تشمل الفيروسات وبرامج التجسس والبرامج الضارة الأخرى التي تستخدم لاختراق الأنظمة وسرقة البيانات.
- أدوات القرصنة: برامج متخصصة تستخدم لاختراق أنظمة الحماية والوصول غير المصرح به إلى الشبكات والأجهزة.
- تقنيات التصيد الاحتيالي: تشمل إنشاء مواقع ورسائل بريد إلكتروني مزيفة لخداع الضحايا وسرقة معلوماتهم الشخصية.
- أدوات إخفاء الهوية: مثل الشبكات الخاصة الافتراضية (VPN) وبرامج التصفح المجهول، التي تستخدم لإخفاء هوية المجرمين.
- برامج التشفير: تستخدم لإخفاء الاتصالات والبيانات الإجرامية عن أعين السلطات.
- منصات الدفع الرقمي والعملات المشفرة: تستخدم لتسهيل المعاملات المالية غير القانونية وغسل الأموال.
- أدوات الهندسة الاجتماعية: تقنيات نفسية تستخدم لخداع الضحايا وجعلهم يكشفون عن معلومات حساسة.
- برامج التحليل والاستغلال: تستخدم لاكتشاف نقاط الضعف في الأنظمة واستغلالها.
- أدوات جمع المعلومات: تستخدم لجمع بيانات عن الأهداف المحتملة من مصادر مفتوحة.
- منصات التواصل المشفرة: تستخدم للتواصل بين المجرمين بطريقة آمنة وصعبة التتبع.

من المهم ملاحظة أن هذه الأدوات تتطور باستمرار مع تطور التكنولوجيا، مما يجعل مكافحة الجريمة الإلكترونية تحدياً مستمراً يتطلب تعاوناً دولياً وتحديثاً مستمراً للأساليب الأمنية.

أشكال الجرائم الإلكترونية

- اقتحام شبكات الحاسب الالي وتخريبها (قرصنة البرامج)
- سرقة المعلومات أو الاطلاع عليها بدون ترخيص
- انتهاك الأعراض وتشويه السمعة
- إتلاف وتغيير ومحو البيانات والمعلومات
- تسريب المعلومات والبيانات
- جمع المعلومات والبيانات وإعادة استخدامها
- نشر واستخدام برامج الحاسب الآلي بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية

هناك عدة أشكال رئيسية للجرائم الإلكترونية، منها:

1. الاختراق والدخول غير المشروع: اقتحام الأنظمة والشبكات بدون إذن للوصول إلى البيانات أو تخريبها.
2. التزوير والاحتيال الإلكتروني: استخدام وسائل إلكترونية للتزوير أو الاحتيال المالي.
3. سرقة الهوية: انتحال شخصية الآخرين عبر الإنترنت لأغراض احتيالية.
4. التصيد الاحتيالي: خداع المستخدمين للحصول على معلوماتهم الشخصية والمالية.
5. نشر البرمجيات الخبيثة: مثل الفيروسات وبرامج الفدية التي تضر بالأنظمة وتشفير البيانات.
6. هجمات الحرمان من الخدمة: تعطيل الخدمات والمواقع الإلكترونية.
7. الجرائم المتعلقة بالمحتوى: مثل نشر المواد الإباحية أو التحريض على العنف.
8. الابتزاز الإلكتروني: تهديد الضحايا بنشر معلومات حساسة للحصول على المال.

تتميز هذه الجرائم بتنوعها وتطورها المستمر مع تقدم التكنولوجيا، مما يشكل تحدياً كبيراً للجهات الأمنية والقانونية.

الباب الثاني
الفصل الأول
أسباب الجريمة الإلكترونية

هناك عدة أسباب أدت إلى انتشار هذا النوع من الجرائم أهمها :

- انتشار البطالة بين فئات الشباب والفقر حيث ان هذه الجرائم معروفة بالكسب السريع وذلك عن طريق التزوير والاحتيال والنصب و انتحال بعض الشخصيات لغرض الحصول على المال .

- الترفيه حيث أن أغلب جرائم السب والشتم والتشهير والقدف كان سببها الترفيه واغلب مرتكبيها من فئة المراهقين دون سن الثانية عشر فما فوق .

- يعلم مرتكبي هذه الجرائم بأنه من الصعب إثبات التهم عليهم وذلك لعدم وجود الخبرة الكافية لدى الجهات الأمنية المسؤولة .

- عدم الوعي الكامل بمخاطر استخدام الانترنت وعدم وضع ضوابط تقيد استخدامه .

مخاطر الجرائم الإلكترونية :

تشمل مخاطر الجرائم الإلكترونية عدة جوانب خطيرة:

1. سرقة البيانات السرية والمعلومات الشخصية، مما قد يؤدي إلى انتهاك الخصوصية وسوء استخدام المعلومات.
2. الخسائر المالية الكبيرة نتيجة اختراق الحسابات البنكية أو الاحتيال الإلكتروني.
3. تلف أنظمة الحاسوب والشبكات بسبب البرامج الضارة والفيروسات.
4. التجسس الإلكتروني، حيث يتم اختراق الأنظمة للوصول إلى معلومات سرية أو مراقبة الأفراد.
5. سرقة الملكية الفكرية وانتهاك العلامات التجارية، مما يضر بالشركات والمؤسسات.
6. فقدان ثقة المستخدمين في التطبيقات والخدمات الإلكترونية.
7. الإضرار بالسمعة للأفراد والشركات على حد سواء.

لذا، من الضروري اتخاذ إجراءات أمنية قوية، مثل استخدام كلمات مرور معقدة وتحديث البرامج باستمرار، للحد من مخاطر هذه الجرائم.

وايضا يؤدي انتشار الجرائم الالكترونية في المجتمعات الى الكثير من المخاطر والتهديدات ومنها المساس بالاقتصاد وتهديد الأمن العام لدول.

وعلى السبيل الأسري المساس بالعلاقات الاسرية وتشكيل الخلافات بين أفراد الأسرة مما يؤدي إلى تفككها وذلك بنشر الإشاعات والاخبار الكاذبة عن بعض شخصيات المجتمع المعروفة او الافراد العاديين .
أصبحت الجرائم الإلكترونية واحدة من أكبر المخاطر التي يتعرض لها مستخدمو الإنترنت حيث تمت سرقة بيانات ملايين المستخدمين للانترنت حول العالم في السنوات الأخيرة .
الجرائم الإلكترونية أصبحت تشكل تهديداً كبيراً لأمن الشركات والمؤسسات ولاصحاب المشاريع وذلك بانتهاك أمن البيانات لهذه المؤسسات وفي اعتقادي أن هذه الجرائم سوف تكون سبباً رئيساً لزيادة وظائف أمن الكمبيوتر والمعلومات إلى ثلاثة أضعافه خلال الخمس السنوات القادمة .

الجهات المستهدفة من قبل الجرائم الإلكترونية :

اولا : الجرائم ضد الأفراد

وتسمي بجرائم الإنترنت الشخصية تتمثل في سرقة الهوية الالكترونية ومنها البريد الالكتروني او انتحال شخصية أخرى بطريقة غير شرعية عبر الانترنت بهدف الاستفادة من ذلك والتضليل وعدم الكشف عن هوية المجرم عند ارتكابه لهذه الجرائم .

تانيا : الجرائم ضد الملكية

تتمثل في نقل البرمجيات الضارة المضمنة في بعض البرامج التطبيقية والخدمية او غيرها بهدف تدمير الاجهزة او البرامج المملوكة للشركات او الاجهزة الحكومية أو البنوك أو حتي الممتلكات الشخصية.

ثالثا : الجرائم ضد الحكومات

مهاجمة المواقع الرسمية وأنظمة الشبكات والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي الهجمات الإرهابية على شبكة الانترنت وهي تتركز على تدمير البنية التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها سياسي .

الفصل الثاني
أنواع الجرائم الإلكترونية

في هذه القائمة سوف نذكر أبرز أنواع الجرائم الإلكترونية :

1. هجمات الحرمان من الخدمات: تعطيل الأنظمة والمواقع الإلكترونية
2. التصيد الاحتيالي: خداع المستخدمين للحصول على معلوماتهم الشخصية
3. برامج الفدية: تشفير بيانات الضحية والمطالبة بفدية لاستعادتها
4. القرصنة: اختراق الأنظمة والحسابات بشكل غير مصرح به
5. سرقة الهوية: انتحال شخصية الضحية لأغراض احتيالية
6. الهندسة الاجتماعية: التلاعب النفسي بالضحايا للحصول على معلومات سرية
7. البرمجيات الخبيثة: مثل الفيروسات وأحصنة طروادة التي تضر بأنظمة الكمبيوتر
8. الابتزاز الإلكتروني: تهديد الضحايا بنشر معلومات خاصة عنهم
9. الاحتيال الإلكتروني: استخدام التكنولوجيا للاحتيال على الأفراد أو الشركات

وفي هذا الخصوص قد حدد الأمن العام السعودي 8 حالات للجرائم الإلكترونية وتشمل :

المساس بالحياة الخاصة للأفراد, انتحال صفة غير صحيحة, إنشاء موقع لمنظمات إرهابية, الاحتيال المالي ,الابتزاز ,التشهير بالآخرين, الوصول إلى بيانات بنكية بطريقة غير شرعية الدخول غير المشروع إلى المواقع الإلكترونية.

(في إطار حملة توعية جديدة لتوعية العموم أطلقت في سنغافورة بموجب الانتربول رسالة مفادها ان الجريمة الالكترونية هي جريمة فعلية وأنه ينبغي -حملها على محمل الجد أسوة بباقي الجرائم)

وقد تناولت الحملة أبرز التهديدات الرئيسية لهذا النوع من الجرائم و صنفتها في التالي :

*التهديد بالاحتيال
*برمجيات انتزاع الفدية
*الابتزاز الجنسي
*القرصنة لتعدين العملات المشفرة
*الاحتيال بالبريد الإلكتروني المهني لتحويل الأموال
*الاعتداءات الجنسية على الأطفال
وقد نبه المسؤول على هذه الحملة مدير مكافحة الجريمة الإلكترونية في الانتربول
((ان الجريمة الالكترونية هي جريمة فعلية واذا وقعتم ضحية لها فسارعوا إلى ابلاغ الشرطة مثلما كنتم ستفعلون لو وقعتم ضحية أي جريمة تقليدية اخرى))

وفي مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية قد نوقشت أهم التدابير لمكافحة الجرائم المتصلة بالحواسيب واهم النقاط التي تناولها المؤتمر كانت حول أن انتشار تكنولوجيا المعلومات والاتصالات الجديدة على نطاق العالم أدي إلى ظهور أشكال أخرى من الجرائم المتصلة بالحواسيب والتي تشكل خطراً على سرية النظم الحاسوبية او سلامتها أو توافرها فحسب وفضلاً على ذلك فإن الابتكارات التكنولوجيا تسفر عن أنماط متمايزة من الابتكار الإجرامي ومن تم فإن الأخطار المختلفة التي تشكلها الجرائم المتصلة بالحواسيب تعكس التباينات بين الطائفة المتنوعة المسماة بالفجوة الرقمية وعن مكافحة هذه الجرائم يواجهون المحققون والمدعون العامون والقضاة على حد السواء عددا من المشاكل المتعلقة بالتحاليل الجنائية تنجم جزئياً عن الطابع غير الملموس للأدلة وسرعة اختفائها وملاحقتها قضائياً غالباً ما يقتضيان تتبع النشاط الإجرامي وآثاره من خلال مجموعة متنوعة من مقدمي خدمات الانترنت.

*** الجرائم الإلكترونية ضمن قوانين بعض الدول**

تختلف قوانين الجرائم الإلكترونية بين الدول، ولكنها تشترك في بعض النقاط الأساسية:

- الأردن: أقر مجلس الأعيان مشروع قانون الجرائم الإلكترونية لسنة 2023، الذي يهدف إلى تحديث التشريعات لمواكبة التطورات التكنولوجية.يشمل القانون عقوبات مالية ويثير جدلاً حول تقييد حرية التعبير على وسائل التواصل الاجتماعي.
- معاهدة الأمم المتحدة: تتضمن مسودة معاهدة الأمم المتحدة لمكافحة الجرائم الإلكترونية أحكاماً قد تجرم التعبير المحمي دولياً، مثل إهانة الأفراد أو الجماعات عبر الإنترنت. تثير هذه الأحكام مخاوف بشأن حقوق الإنسان وحرية التعبير.
- التعاون الدولي: يعتمد التعاون الدولي في مكافحة الجرائم الإلكترونية على معاهدات ثنائية وإقليمية ومتعددة الأطراف، التي تسهل تبادل الأدلة والمعلومات بين الدول.

اغلب الدول قد صادقت على القانون الخاص بالجرائم الالكترونية وفرض عقوبات ماعاد بعض الدول بالرغم من ان الاتحاد الافريقي قد اعتمد في عام 2014 اتفاقية بشأن أمن القضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي لم تتم مصادقتها بحلول كانون الثاني \ يناير 2020 إلا اربعة دول من أصل الـ 55 الأعضاء في الاتحاد الأفريقي.
ويفيد التقرير بأن هذا الأمر يبين أن العديد من البلدان الأفريقية مازالت الجريمة الالكترونية مسألة غير حتمية ما يزيد من تفاقم المشكلة.

ما هو دور الولايات المتحدة والمملكة المتحدة في مواجهة الجرائم الإلكترونية ؟
إن الولايات المتحدة والمملكة المتحدة رائدتان في الحرب العالمية ضد الجرائم الإلكترونية وهما ملتزمتان باستخدام جميع السلطات المتاحة للدفاع ضد التهديدات الإلكترونية.
حيث تتعرض الدولتان لهجوم إلكتروني يهدد أمنهم واستقرارهم وأصابع الاتهام موجهة لروسيا.

أشهر الجرائم الإلكترونية:

في ظل التطور الكبير في المجال الالكتروني التكنولوجي كان النصيب الأكبر للإنترنت من هذا التطور ولكن لم يقتصر الأمر على الجانب الإيجابي بل انعكس أيضا بالسلب علي هذا العالم الافتراضي ومستخدميه فأصبح سلاح ذو حدين.

فإذا ما أحسنا استخدام الإنترنت بالشكل الصحيح كان ذلك العالم الافتراضي مثالي لاعيب فيه أما من لا يضع قيود وقوانين وعقوبات على كل من يسئ استخدامه فقد يجره ذلك للوقوع في شرور المجرمين الالكترونيين الأمر الذي يعود عليه بكوارث .

علي الرغم من أن عدد الجرائم الالكترونية اصبح كبير جداً بشكل لا يمكن تصديقه إلا أنه هناك بعض الحوادث والجرائم الإلكترونية الأكثر شهرة في العالم والتي لا يزال الحديث عنها إلى يومنا هذا لشدة ضخامتها و الضربة القاسية التي وجهت لها ومن أشهرها :

- **الهجوم الإلكتروني على شركة التأمين الأمريكية Anthem** تعرضت شركة التأمين الأمريكية في عام 2015 لهجوم إلكتروني مباغت استهدف معلومات المستخدمين والعملاء الموجودين بالشركة والبالغ عددهم حوالي ثمانون مليون عميل الأمر الذي تسبب في سرقة وتسريب بياناتهم الشخصية والسرية التي كانت موجودة لدى شركة التأمين .

وبكل اسف الشركة لم تستطع أن توقف هذه الجريمة الإلكترونية التي نتج عنها رفع الألف من الدعوى القضائية عليها وقدرت خسارتها بسبب هذه الجريمة الغير معروف مرتكبها بحوالي مئة مليون دولار أمريكي.

- **اختراق شركة سوني sony** حيث تعرضت شركة سوني اليابانية لا اختراق خطير من قبل مخترقين يدعو ب (حراس السلام) **peace Guardians of** قاموا بزرع فيروس خبيث في خوادم الشركة مما تسبب في تسرب بيانات عملاء أصحاب الشركة ومحادثات لهم بالإضافة لسيطرة المخترقين على معلومات مهمة جدا تخطي استراتيجية شركة سوني التسويقية بالإضافة لمجموعة قامت شركة سوني بانتاجها.

ويذكر البعض أن السبب وراء قيام المخترقين بهذا الفعل هو إنتاج لشركة لفيلم أمريكي The interview يستهزئ برئيس كوريا الشمالية حيث يتم اتهام رئيس كوريا انذاك بانه وراء هذا الاختراق ومن أشهر الجرائم ايضا:

- هجوم الكتروني ضرب قاعدة بيانات المتقاعدين العسكريين الامريكان.
- الهجوم الالكتروني على قاعدة بيانات متاجر Target المالية وهو أكبر المتاجر في الولايات المتحدة الأمريكية.
- ويعد الاختراق الكبير لوكالة ناسا للفضاء من أكبر الجرائم الإلكترونية.

تشمل الأمثلة الشهيرة على الجرائم الإلكترونية التي حدثت في السنوات الأخيرة:

1. اختراق تويتر (X): في عام 2023، تم اختراق 220 مليون سجل من تويتر.
2. هجوم على Hot Topic: في أغسطس 2023، تم اكتشاف محاولات غير مصرح بها للوصول إلى حسابات العملاء.
3. هجوم الفدية على Prospect Medical: في أغسطس 2023، أُجبرت عدة مرافق طبية على الإغلاق بسبب هجوم فدية.
4. هجوم DDoS على البرلمان الفنلندي: في أغسطس 2022، تعرض موقع البرلمان لهجوم.

بعض الأمثلة العامة لضحايا الجرائم الإلكترونية:

1. أشخاص تحولت حياتهم وحياة أسرهم إلى جحيم بسبب وقوعهم ضحية للجرائم الإلكترونية، نتيجة عدم معرفتهم بأبسط إجراءات الوقاية من الاختراق.
2. ضحايا التصيد الاحتيالي الذين يقعون في فخ فتح روابط في رسائل البريد الإلكتروني العشوائية أو المواقع الإلكترونية غير المألوفة، مما يؤدي إلى سرقة بياناتهم الشخصية.
3. أفراد يتعرضون للابتزاز الجنسي، خاصة الفتيات، حيث يهددهن المجرمون بنشر صور أو فيديوهات خاصة إذا رفضن إقامة علاقات غير شرعية معهم.
4. ضحايا التصيد بالحربة، وهي حملات تصيد احتيالي مستهدفة تحاول خداع أفراد معينين لتعريض أمن المؤسسات التي يعملون فيها للخطر.
5. أشخاص يقعون ضحية لهجمات البرمجيات الخبيثة، مما يؤدي إلى سرقة بياناتهم السرية أو استخدام أجهزتهم لتنفيذ أعمال إجرامية أخرى.

رغم عدم وجود قصص محددة لضحايا الجرائم الإلكترونية إلا أن هذه الأمثلة تعكس الأنماط الشائعة للجرائم الإلكترونية وتأثيرها على الضحايا. من المهم التأكيد على ضرورة الوعي بهذه المخاطر واتخاذ إجراءات الحماية اللازمة.

الفصل الثالث

السب والشتم والقذف في وسائل التواصل الاجتماعي

يعد السب والشتم والقذف عبر وسائل التواصل الاجتماعي من الجرائم الإلكترونية الخطيرة التي تنتشر بشكل متزايد في العصر الرقمي. وفيما يلي بعض النقاط الهامة حول هذه الظاهرة:

1. تعتبر هذه الأفعال جرائم يعاقب عليها القانون في معظم الدول، حيث تندرج تحت جرائم السب والقذف الإلكتروني.
2. يمكن أن تؤدي إلى عقوبات تشمل الغرامات المالية والسجن، اعتماداً على خطورة الحالة وقوانين كل دولة.
3. تسبب هذه الأفعال أضراراً نفسية واجتماعية كبيرة للضحايا، خاصة مع سرعة انتشار المحتوى عبر الإنترنت.
4. من المهم توثيق وتصوير أي حالات سب أو قذف للاحتفاظ بها كأدلة في حال تقديم شكوى قانونية.
5. ينصح بتجنب الرد على الإساءات بالمثل، وبدلاً من ذلك استخدام خيارات الإبلاغ والحظر المتاحة على منصات التواصل الاجتماعي.
6. التوعية بخطورة هذه الأفعال وعواقبها القانونية أمر ضروري، خاصة بين فئة الشباب.
7. على الرغم من صعوبة السيطرة الكاملة على هذه الظاهرة، إلا أن تطبيق القوانين بصرامة وزيادة الوعي يمكن أن يساهم في الحد منها.

أسباب انتشار الشتم والسب في وسائل التواصل الاجتماعي :

1. إخفاء الهوية: توفر وسائل التواصل الاجتماعي درجة من عدم الكشف عن الهوية، مما قد يشجع البعض على التصرف بطريقة غير لائقة دون خوف من العواقب المباشرة.
2. غياب التواصل المباشر: عدم وجود تفاعل وجهاً لوجه قد يقلل من التعاطف والشعور بمشاعر الآخرين.

3. سهولة التعبير: توفر هذه المنصات وسيلة سهلة وسريعة للتعبير عن الغضب أو الإحباط دون تفكير في العواقب.
4. انتشار الشائعات: سرعة انتشار المعلومات قد تؤدي إلى ردود فعل عاطفية وغير مدروسة.
5. ضعف الرقابة: صعوبة مراقبة جميع المحتويات بشكل فعال قد يشجع على السلوك غير اللائق.
6. التأثر بسلوك الآخرين: رؤية الآخرين يتصرفون بطريقة غير لائقة قد يشجع على تقليد هذا السلوك.
7. قلة الوعي بالعواقب القانونية: عدم إدراك أن السب والشتم عبر الإنترنت قد يكون له عواقب قانونية.

من المهم زيادة الوعي بخطورة هذه الظاهرة وتعزيز ثقافة الاحترام والتعامل الإيجابي عبر الإنترنت.

قوانين و تنظيمات تحمي المستخدمين من السب والشتم على وسائل التواصل الاجتماعي

هناك قوانين وتنظيمات في العديد من الدول تهدف إلى حماية المستخدمين من السب والشتم على وسائل التواصل الاجتماعي:

1. قوانين مكافحة التنمر الإلكتروني: تجرم هذه القوانين المضايقات والتهديدات عبر الإنترنت.
2. قوانين القذف والتشهير: تحمي الأفراد من الادعاءات الكاذبة التي تضر بسمعتهم.
3. قوانين حماية الخصوصية: تمنع نشر المعلومات الشخصية دون إذن.
4. قوانين مكافحة خطاب الكراهية: تحظر التحريض على العنف أو التمييز ضد فئات معينة.
5. سياسات المنصات: تضع شركات التواصل الاجتماعي قواعد سلوك تحظر المحتوى المسيء.
6. آليات الإبلاغ: توفر المنصات أدوات للمستخدمين للإبلاغ عن المحتوى المسيء.
7. عقوبات رادعة: تفرض بعض الدول غرامات وعقوبات على مرتكبي الإساءات الإلكترونية.

رغم وجود هذه القوانين، يبقى التحدي في تطبيقها بفعالية نظراً لطبيعة الإنترنت العابرة للحدود وصعوبة تتبع المسيئين في بعض الحالات.

العقوبات القانونية التي تنتظر كل من يسب أو يشتم على وسائل التواصل الاجتماعي

العقوبات تختلف من دولة لأخرى و تشمل:

1. غرامات مالية تتراوح قيمتها حسب شدة المخالفة وقوانين كل دولة.
2. عقوبات السجن في الحالات الشديدة أو المتكررة.
3. تعليق أو إغلاق حسابات المخالفين على منصات التواصل الاجتماعي.
4. الإلزام بتقديم اعتذار علني للطرف المتضرر.
5. دفع تعويضات مدنية للضحية في حال رفع دعوى قضائية.

من المهم الإشارة إلى أن شدة العقوبة تعتمد على عدة عوامل مثل طبيعة المحتوى المسيء، تكرار المخالفة، والضرر الناتج عن الفعل كما أن القوانين تختلف بين الدول.

الباب الثالث

الفصل الأول

مكافحة الجرائم الالكترونية بالقانون الليبي

تم إصدار القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا

هذا القانون صدر عن مجلس النواب الليبي في 27 سبتمبر 2022 يهدف القانون إلى مكافحة مختلف أنواع الجرائم الإلكترونية في ليبيا يتضمن

القانون تعريفات لمصطلحات مهمة مثل أدوات التعريف والهوية الرقمية، النقود الإلكترونية، والبطاقات المصرفية الإلكترونية

يعاقب القانون على بعض الأفعال مثل مزج أو تركيب الصوت أو الصورة لأحد الأشخاص باستخدام شبكة المعلومات دون تصريح، بعقوبة الحبس لمدة لا تقل عن سنة

يرتبط هذا القانون بقطاعات الأمن والاتصالات وتقنية المعلومات، ويتعلق بشكل خاص بالأمن الرقمي

الجرائم الإلكترونية التي يغطيها القانون رقم 5 لسنة 2022

يغطي القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا عدة أنواع من الجرائم الإلكترونية، منها

الدخول غير المصرح به إلى المواقع الإلكترونية وأنظمة المعلومات الرقمية، أو إلغاؤها أو حذفها أو إتلافها أو تعطيلها أو تعديلها أو نقل أو نسخ بياناتها دون موافقة مكتوبة أو إلكترونية صريحة من مالكها

تهديد الأمن أو السلامة العامة باستخدام وسائل إلكترونية، حيث يعاقب القانون على هذه الجريمة بالسجن مدة لا تقل عن خمس سنوات وبغرامة لا تقل عن 10,000 دينار ولا تزيد على 100,000 دينار ليبي

مزج أو تركيب الصوت أو الصورة لأحد الأشخاص باستخدام شبكة المعلومات دون تصريح، ويعاقب عليها بعقوبة الحبس لمدة لا تقل عن سنة

الجرائم المتعلقة بأدوات التعريف والهوية الرقمية، والنقود الإلكترونية، والبطاقات المصرفية الإلكترونية الالتقاط أو الاعتراض غير المشروع للبيانات أو المعلومات

يبدو أن القانون يهدف إلى تغطية مجموعة واسعة من الجرائم الإلكترونية، بما في ذلك الاختراق، والاحتيال الإلكتروني، وانتهاك الخصوصية، وتهديد الأمن العام عبر الوسائل الإلكترونية. هذا القانون يمثل جزءاً من جهود ليبيا لمواكبة التطورات التكنولوجية وحماية مواطنيها من الجرائم الإلكتروني

الأخطاء التي تعتري القانون رقم 5 لسنة 2022

تعريفات فضفاضة

يستخدم القانون تعريفات غامضة وفضفاضة مثل "الآداب العامة" و"النعرات العنصرية الجهوية" دون تحديد واضح، مما يفتح المجال لملاحقة التعبير السلمي

سلطات واسعة للمراقبة

يمنح القانون "الهيئة الوطنية لأمن وسلامة المعلومات" سلطات واسعة لمراقبة الاتصال والمحتوى على الإنترنت دون أوامر قضائية في حالات "المتطلبات الأمنية أو العاجلة"، انتهاكاً الخصوصية

حظر المحتوى دون ضوابط

يسمح القانون للهيئة بحظر المحتوى الذي تعتبره مخالفاً للآداب العامة أو يحتوي على "نعرات عنصرية" دون تعريف واضح أو إجراءات قانونية

عقوبات قاسية

ينص القانون على عقوبات بالسجن وغرامات مالية كبيرة لمجرد الإبلاغ عن الجرائم الإلكترونية أو الشروع فيها

لذلك، تعتبر منظمات حقوقية مثل هيومن رايتس ووتش أن هذا القانون قمعي ويهدد حرية التعبير والخصوصية على الإنترنت في ليبيا

و في اخر عملية بحث قمت بها , لا يبدو أن هناك تغييرات جوهرية تم إدخالها على القانون الليبي رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية منذ إقراره ومع ذلك، يمكن الاشارة إلى بعض النقاط التالية

تم تخفيف بعض العقوبات مثل إزالة عقوبة السجن لمدة 5 سنوات لجريمة "مزج أو تركيب الصور أو الأصوات الإباحية ونشرها

لم يتم الأخذ بمطالب منظمات المجتمع المدني والخبراء بتعديل المواد المثيرة للجدل مثل التعريفات الفضفاضة وسلطات المراقبة الواسعة للهيئة الوطنية

أصر مجلس النواب على إقرار القانون رغم الانتقادات الواسعة من منظمات حقوقية دولية مثل هيومن رايتس ووتش واكسس ناو بسبب تهديده لحرية التعبير والخصوصية

لم يتم إجراء تعديلات جوهرية على القانون منذ إقراره، حيث ظل يحتوي على مواد قمعية تجرم التعبير السلمي وتسمح بالمراقبة الواسعة دون ضوابط كافية

لذلك، يبدو أن القانون الليبي لمكافحة الجرائم الإلكترونية لا يزال يواجه انتقادات واسعة من المنظمات الحقوقية لاحتوائه على مواد تهدد الحريات الأساسية على الإنترنت دون إجراء تعديلات جوهرية عليه حتى الآن

بحسب القانون الليبي رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، تتمتع الهيئة الوطنية لأمن وسلامة المعلومات بسلطات واسعة، منها

سلطة المراقبة والاعتراض

تملك الهيئة صلاحية "مشاهدة البيانات أو المعلومات أو الحصول عليها" أو ما يعرف بـ"الاعتراض" وفقًا للمادة 1 من القانون، دون الحاجة لأوامر قضائية في حالات المتطلبات الأمنية أو العاجلة

سلطة حجب المحتوى

تستطيع الهيئة حسب المادة 7 "حجب كل ما ينشر النعرات أو الأفكار التي من شأنها زعزعة أمن المجتمع واستقراره والمساس بسلمه الاجتماعي" دون تحديد واضح لهذه المصطلحات

سلطة التنصت

يحق للهيئة "التنصت أو التقاط أو تسجيل أو نقل أو بث المحادثات

لذلك، تعتبر منظمات حقوقية مثل هيومن رايتس ووتش واكسس ناو أن هذه الصلاحيات الواسعة للهيئة تهدد حرية التعبير والخصوصية على الإنترنت في ليبيا لغياب الضوابط والرقابة القضائية الكافية

المهام الرئيسية للهيئة الوطنية لأمن وسلامة المعلومات في ليبيا تشمل

مراقبة الشبكة الوطنية وأمنها

تقوم الهيئة بمراقبة الشبكة الوطنية وتحسين أدائها والتأكد من سلامتها ومطابقتها للمعايير المعتمدة دولياً

توفير الحلول الأمنية

تقدم الهيئة الحلول الأمنية المرتبطة بطبيعة عملها مثل تصميم الجدران النارية وأجهزة كشف ومنع الاختراق ومضادات الفيروسات

تقييم الشبكات والأنظمة وإصدار شهادات

تقوم الهيئة بتقييم ومراجعة الشبكات والأنظمة في المؤسسات الحكومية والخاصة وإصدار شهادات الجودة وفقاً للمعايير الدولية

وضع السياسات والمعايير الأمنية

تضع الهيئة السياسات والمعايير المرتبطة بأمن وسلامة المعلومات والاتصالات بالإضافة إلى التعريفات والإرشادات اللازمة

التنصت والاعتراض على الاتصالات

وفقاً للقانون، يحق للهيئة التنصت أو التقاط أو تسجيل المحادثات الخاصة في إطار مكافحة الجرائم الإلكترونية

لذلك، تتمتع الهيئة بصلاحيات واسعة في مراقبة الشبكات والاتصالات وفرض الحلول الأمنية، إلى جانب وضع السياسات والمعايير ذات الصلة

تطبيق قانون مكافحة الجرائم الإلكترونية الليبي رقم 5 لسنة 2022 يمكن أن ينتج عنه عدة مخاطر على النشاطات الإلكترونية:

1. **انتهاك الخصوصية:** يمنح القانون الهيئة الوطنية لأمن وسلامة المعلومات سلطات واسعة لمراقبة الاتصالات الإلكترونية وحجب المواقع، مما قد ينتهك الحق في الخصوصية.
2. **تقييد حرية التعبير**: يفرض القانون عقوبات مشددة على بعض الأنشطة عبر الإنترنت، مما قد يقيد حرية التعبير ويستهدف النشطاء والمدافعين عن حقوق الإنسان.
3. **استخدام تعسفي**: استخدام صياغات وتعريفات فضفاضة وغامضة لبعض المواد قد يؤدي إلى إساءة استخدامها وتفسيرها بشكل تعسفي، مما يتيح للسلطات استهداف المعارضة والنشطاء.
4. **تأثير سلبي على المجتمع المدني**: قد يؤثر القانون سلباً على عمل منظمات المجتمع المدني في توثيق انتهاكات حقوق الإنسان، ويحد من قدرتها على العمل بحرية وأمان.
5. **ضعف النظام القضائي:** نظام العدالة في ليبيا ضعيف وغير فعال، مما يزيد من مخاطر إساءة استخدام القانون دون رقابة فعالة أو ضمانات قانونية مناسبة.

الآثار الاقتصادية المحتملة لتطبيق هذا القانون

تطبيق قانون مكافحة الجرائم الإلكترونية الليبي رقم 5 لسنة 2022 يمكن أن يكون له عدة آثار اقتصادية محتملة:

1. **تقييد الاستثمار**: قد يؤدي القانون إلى تقييد حرية الإنترنت، مما يجعل ليبيا بيئة أقل جاذبية للاستثمار الأجنبي في قطاع التكنولوجيا والاتصالات.
2. **زيادة التكاليف التشغيلية**: الشركات قد تحتاج إلى استثمار مبالغ كبيرة في تحسين أنظمة الأمان الإلكتروني والامتثال للقوانين الجديدة، مما يزيد من تكاليف التشغيل.
3. **تأثير سلبي على الابتكار**: القيود الصارمة قد تعيق الابتكار وتطوير الأعمال الرقمية، مما يؤثر سلباً على النمو الاقتصادي في هذا القطاع.
4. **تأثير على التجارة الإلكترونية:** قد يؤدي القانون إلى تقليل الثقة في التجارة الإلكترونية، مما يؤثر على الشركات التي تعتمد على الإنترنت لتقديم خدماتها ومنتجاتها.
5. **تأثير على الشركات الصغيرة والمتوسطة**: الشركات الصغيرة والمتوسطة قد تجد صعوبة في الامتثال للمتطلبات الجديدة، مما قد يؤدي إلى خروجها من السوق أو تقليل نشاطها.

- **تعريف القانون الليبي للجريمة الالكترونية** : هي كل فعل يرتكب من خلال أستخدام أنظمة الحاسوب الألي او شبكة المعلومات الدولية أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون٠

تعريف القانون الليبي لبعض المصطلحات الواردة به و الخاصة بالمعاملات الالكترونية:

- **الاختراق** هو القدرة على الوصول إلى أي وسيلة تقنية معلوماتية بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاصة.

- **القرصنة الإلكترونية** الاستخدام أو النسخ غير مشروع لنظم التشغيل والبرامج الحاسوبية المختلفة في نظام الحماية الخاصة.

- **التشفير** عملية تحويل البيانات الالكترونية الى رموز غير معروفة او غير مفهومة يستحيل قرائتها او معرفتها دون إعادتها الى هيئتها الأصلية.

- **إعاقة الوصول إلى الخدمة أو التشويش عليها** هو إدراك الخدمة وتشمل السيطرة على العمل وحركته بشكل صحيح.

- **الدليل الجنائي الرقمي** هو نتائج تحليل من أنظمة الحاسوب أو شبكات الاتصال او أجهزة التخزين الرقمية بمختلف انواعها.

- **الهوية الرقمية** هي تمثيل رقمي لمعلومات الفرد داخل المجتمع على المعلومات الدولية بالصيغة التي اعتمدها هذا الفرد والمتوقعة من قبل الآخرين وقد يكون للفرد أو للجهة هويات رقمية متعددة في المجتمعات الالكترونية المتعددة.

- **ادوات التعريف والهوية** أي آلية ونظام رقمي أو أداة رقمية تستخدم لتمثيل الهوية الرقمية للأفراد التي تمكنهم من العمل بطريقة آمنة مع واجهات استخدام متناسقة على الأنظمة المختلفة على المعلومات الدولية.

- **النقود الإلكترونية** هي قيمة نقدية مخزنة على وسيلة إلكترونية مدفوعة مقدماً وغير مرتبطة بحساب مصرفي وتحظى بقبول واسع يستعمل كأداة للدفع لتحقيق أغراض مختلفة.

- **البطاقة المصرفية** أداة صادرة عن مصرف أو مؤسسة تتيح لصاحبها سحب الاموال وتحويلها.

- **الالتقاط أو الاعتراض** مشاهدة البيانات أو المعلومات أو الحصول عليها.

الهيئة الوطنية لأمن وسلامة المعلومات المنشأة بموجب قرار مجلس الوزراء رقم 28 لسنة 2013
تسري أحكام هذا القانون على أي من الجرائم المنصوص عليها فيه إذا ارتكبت جميعها أو بعضها داخل ليبيا ,أو ارتكبت كل افعالها خارج ليبيا وامتدت نتائجها وآثارها داخل ليبيا لو لم يكن معاقباً عليها في الدولة التي ارتكبت فيها.

أهداف القانون

يهدف القانون إلى حماية التعاملات الإلكترونية، والحد من وقوع الجرائم الإلكترونية وذلك بتحديد هذه الجرائم و إقرار العقوبات الرادعة لها، وبما يؤدي إلى تحقيق ما يلي:

1. المساعدة على تحقيق العدالة والأمن المعلوماتي.
2. حماية النظام العام والآداب العامة.
3. حماية الاقتصاد الوطني.
4. حفظ الحقوق المترتبة على الاستخدام المشروع لوسائل التقنية الحديثة.
5. تعزيز الثقة العامة في صحة وسلامة المعاملات الإلكتروني.

عقوبة عدم التبليغ عن مرتكبي الجريمة الإلكترونية

يعاقب بالحبس وبغرامة لا تزيد عن 3,000 ثلاثة آلاف دينار ليبي كل من علم بارتكاب أي من الجرائم المنصوص عليها في القانون رقم 5 لسنة 2022م الخاص بالجرائم الالكترونية الليبي ولم يقم بالتبليغ عن مرتكبها.
وتكون العقوبة الحبس مدة لا تقل عن ستة أشهر والغرامة لا تقل عن 3,000 ثلاثة آلاف دينار ليبي ولا تزيد عن 5,000 خمسة آلاف دينار ليبي اذا كان الجاني موظفاً عاماً او مكلفاً بخدمة عامة ووقعت الجريمة نتيجة إخلاله بواجبات ما كلف به.
الاستثناء في هذا القانون انه يجوز للمحكمة الإعفاء من هذه العقوبة إذا كان من امتنع عن الإبلاغ زوج للجاني أو احد أصوله أو فروعه أو أحد أخوته.

لقد تم صياغة القانون بموجب قرار مجلس النواب رقم 28 لسنة 2013م

الفصل الثاني

السب والشتم والقذف في القانون رقم 5 لسنة 2022 للجرائم الإلكترونية

فالبداية لابد من التفريق بين السب والشتم والقذف في القانون الليبي وقانون الجرائم الإلكترونية:

السب : نصت عليه المادة 438 عقوبات بأن كل شخص يخدش شرف شخص أو اعتباره في حضوره يعاقب بالحبس مدة لا تزيد عن 6 أشهر وبغرامة لا تزيد عن 25 دينار.

الشتم :هو الذم والاساءة بالقول ويكون لمرة واحدة في حضور المخاطب.

القذف : هو الرمي بالزنا او نفي النسب باي طريقة كانت وفي حضور المقذوف أو غيبته وفي علانية أو بدونها يعاقب بالجلد حداً ثمانين جلدة ولاتقبل له شهادة كل من ثبت عليه ارتكاب هذه الجريمة.

السب والشتم والقذف في وسائل التواصل الاجتماعي

العقوبة الأساسية لجريمة السب و القذف في وسائل التواصل الاجتماعي هي السجن لمدة تتراوح بين سنة الى 4 سنوات أو غرامة مالية وقد يتم زيادة هذه العقوبة في بعض الحالات أو سيتم تخفيضها و احياناً لا يتم فرض أي عقوبة في اعتقادي ان هناك خلط كبير بين هذه الجرائم وبين حرية التعبير ولا اعلم تماماً ما هو هدف المشرع لعدم طرحه لنص خاص بهذه الجريمة التي ترتكب بشكل يومي في حق الكثير من مستخدمي مواقع التواصل الاجتماعي.

الخلاصة:

لا يتناول قانون رقم 5 لسنة 2022 جرائم السب والشتم والقدف وبالتالي لا يحدد عقوبات لها. العقوبات المتعلقة بالسب والشتم تُحدد في قوانين مكافحة جرائم تقنية المعلومات لدول أخري، والتي تعاقب على هذه الجرائم بالحبس والغرامة.

التحديات التي تواجه تنفيذ القانون رقم 5 لسنة 2022 في ليبيا

التحديات المحتملة التي قد تواجه تنفيذ القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا:

1. **التطور السريع للتكنولوجيا:** قد يجعل من الصعب على القانون مواكبة الأساليب الجديدة للجرائم الإلكترونية.
2. **نقص الخبرات التقنية:** قد تفتقر الجهات المعنية بتنفيذ القانون إلى الخبرات التقنية اللازمة للتعامل مع الجرائم الإلكترونية المعقدة.
3. **صعوبات في جمع الأدلة الرقمية:** قد يكون من الصعب جمع وحفظ الأدلة الرقمية بطريقة تضمن قبولها في المحاكم.
4. **التحديات عبر الحدود:** نظراً لطبيعة الجرائم الإلكترونية العابرة للحدود، قد تكون هناك صعوبات في التعاون الدولي لمكافحتها.
5. **الموازنة بين الأمن والخصوصية:** قد يكون من الصعب تحقيق التوازن بين مكافحة الجرائم وحماية خصوصية المواطنين.
6. **الوعي العام:** قد يكون هناك نقص في الوعي العام بالجرائم الإلكترونية وكيفية الإبلاغ عنها.
7. **البنية التحتية:** قد تكون هناك تحديات تتعلق بتوفير البنية التحتية اللازمة لتنفيذ القانون بفعالية.
8. **التحديات السياسية والأمنية:** الوضع السياسي والأمني غير المستقر في ليبيا قد يؤثر على تنفيذ القانون بشكل فعال.

هذه التحديات تستدعي جهوداً متواصلة لتطوير القدرات التقنية والقانونية، وزيادة الوعي العام، وتعزيز التعاون الدولي في مجال مكافحة الجرائم الإلكترونية.

حرية التعبير بالقانون رقم 5 لسنة 2022

حرية التعبير في سياق القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا:

1. القانون يهدف إلى حماية المعاملات الإلكترونية وأمن المعلومات، لكنه قد يثير مخاوف بشأن حرية التعبير.
2. المادة 6 من القانون تتعلق بحماية حقوق الملكية الفكرية للأعمال الأدبية والفنية والعلمية المنشورة عبر الإنترنت، مما قد يؤثر على حرية التعبير الإبداعي.
3. المادة 7 تنص على مراقبة ما ينشر عبر وسائل التقنية الحديثة، وهذا قد يثير مخاوف بشأن الرقابة وتقييد حرية التعبير.

4. هناك مخاوف عامة من قبل منظمات حقوقية دولية حول استخدام قانون الجرائم الإلكترونية الليبي لاستهداف النشطاء والمعارضين السياسيين.
5. المنظمات الحقوقية تدعو إلى ضرورة وجود تعريفات واضحة ومحددة في مثل هذه القوانين لتجنب إساءة استخدامها لقمع حرية التعبير.
6. هناك دعوات لإشراك المجتمع المدني والمنظمات غير الحكومية في صياغة ومراجعة مثل هذه القوانين لضمان حماية الحقوق الأساسية.
7. من المهم الموازنة بين متطلبات الأمن السيبراني وحماية حرية التعبير والحقوق الرقمية للمواطنين.

في ضوء هذه النقاط، يبدو أن هناك حاجة لمزيد من الشفافية والنقاش العام حول تأثير هذا القانون على حرية التعبير في ليبيا، وضمان وجود ضمانات كافية لحماية هذا الحق الأساسي.

القواعد الدولية لحرية التعبير والرأي في قانون الجرائم الإلكترونية :

النقاط الرئيسية حول القواعد الدولية لحرية التعبير والرأي في سياق قوانين الجرائم الإلكترونية:

1. **ضرورة احترام الحق في حرية التعبير والرأي:** يجب أن تحترم قوانين الجرائم الإلكترونية الحق الأساسي في حرية التعبير والرأي، كما هو منصوص عليه في المواثيق الدولية لحقوق الإنسان.
2. **تجنب الصياغات الفضفاضة والغامضة:** ينبغي أن تكون نصوص القانون واضحة ومحددة لتجنب إساءة استخدامها لقمع حرية التعبير.
3. **عدم استخدام القانون لاستهداف المعارضين:** يجب ألا تُستخدم قوانين الجرائم الإلكترونية كأداة لاستهداف النشطاء أو المنتقدين للحكومات.
4. **ضمان الرقابة القضائية:** يجب أن تخضع أي إجراءات لمراقبة أو حجب المحتوى الإلكتروني لإشراف قضائي مستقل.
5. **التوازن بين الأمن وحقوق الإنسان:** ينبغي تحقيق توازن دقيق بين متطلبات الأمن السيبراني وحماية حقوق الإنسان الأساسية.
6. **المشاركة المجتمعية:** ضرورة إشراك منظمات المجتمع المدني والخبراء في صياغة ومراجعة قوانين الجرائم الإلكترونية.
7. **الشفافية:** يجب أن تكون عملية صياغة وتطبيق القوانين شفافة وخاضعة للمساءلة.
8. **تجنب الرقابة الشاملة:** عدم السماح بالرقابة الشاملة على الفضاء الرقمي دون إذن قضائي.
9. **حماية الخصوصية:** ضمان حماية الحق في الخصوصية وحماية البيانات الشخصية.
10. **الامتثال للمعايير الدولية:** ضرورة أن تتوافق القوانين المحلية مع الالتزامات الدولية للدول في مجال حقوق الإنسان.

هذه القواعد تهدف إلى ضمان أن تكون قوانين الجرائم الإلكترونية أداة لحماية الأمن السيبراني دون المساس بالحقوق الأساسية للمواطنين، وخاصة حرية التعبير والرأي.

المخاطر المحتملة للفنانين والكتاب في ليبيا نتيجة تطبيق القانون رقم 5 لسنة 2022

ومن هنا يمكن تحديد بعض المخاطر المحتملة للفنانين والكتاب في ليبيا نتيجة تطبيق القانون رقم 5 لسنة 2022:

1. **تقييد حرية التعبير الإبداعي:** المادة 6 من القانون تتعلق بحماية حقوق الملكية الفكرية للأعمال الأدبية والفنية والعلمية المنشورة عبر الإنترنت، مما قد يؤدي إلى تفسيرات مقيدة لما يمكن نشره أو مشاركته.
2. **الرقابة المحتملة:** المادة 7 تنص على مراقبة ما ينشر عبر وسائل التقنية الحديثة، مما قد يؤدي إلى رقابة على الأعمال الفنية والأدبية.
3. **إمكانية الاستهداف:** هناك مخاوف من استخدام القانون لاستهداف الأعمال الأدبية أو الفنية التي تنتقد السلطات أو تتناول مواضيع حساسة.
4. **تقييد الوصول إلى المعلومات:** قد يؤدي القانون إلى تقييد الوصول إلى بعض الأعمال الفنية أو الأدبية بحجة حماية الأمن القومي أو النظام العام.
5. **الحد من التبادل الثقافي:** قد يؤدي تطبيق القانون بشكل صارم إلى الحد من التبادل الثقافي عبر الإنترنت مع المجتمع الدولي.
6. **غموض في التعريفات:** عدم وجود تعريفات واضحة ومحددة في القانون قد يؤدي إلى تفسيرات واسعة تستخدم لتقييد نشر بعض الأعمال الإبداعية.
7. **المساس بالحق في الخصوصية:** القانون قد يؤثر على الحق في الخصوصية وحماية المعطيات الشخصية للفنانين والكتاب.
8. **إمكانية الحجب:** القانون يمنح إمكانية حجب المواقع والمحتوى، مما قد يؤثر على نشر وتوزيع الأعمال الفنية والأدبية.

هذه المخاطر تثير مخاوف جدية بشأن تأثير القانون على حرية التعبير والإبداع في ليبيا، وقد دفعت منظمات حقوقية إلى المطالبة بإلغاء القانون أو تعديله لضمان حماية الحقوق الأساسية.

المخاطر التي يمكن أن تتعرض لها الحريات الفردية نتيجة تطبيق القانون رقم 5 لسنة 2022

مخاطر محتملة على الحريات الفردية نتيجة تطبيق القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا:

1. **تقييد حرية التعبير والرأي:** القانون قد يستخدم لتقييد حرية التعبير والرأي على الإنترنت، خاصة فيما يتعلق بانتقاد السلطات أو مناقشة مواضيع حساسة.
2. **المساس بالحق في الخصوصية:** القانون يمنح صلاحيات واسعة لمراقبة ما ينشر عبر وسائل التقنية الحديثة، مما قد يؤدي إلى انتهاك خصوصية المستخدمين.
3. **تقييد حرية التجمع السلمي:** قد يستخدم القانون لتقييد التنظيم والتواصل عبر الإنترنت لأغراض التجمع السلمي.
4. **الرقابة الشاملة:** القانون يقنن الرقابة الشاملة للسلطة التنفيذية على الفضاء الرقمي دون إذن قضائي.
5. **إمكانية حجب المواقع والمحتوى:** القانون يمنح السلطات إمكانية حجب المواقع والمحتوى، مما قد يؤدي إلى تقييد الوصول إلى المعلومات.
6. **استهداف النشطاء والمعارضين:** هناك مخاوف من استخدام القانون لاستهداف النشطاء والمعارضين السياسيين.
7. **غموض في التعريفات:** عدم وجود تعريفات واضحة ومحددة في القانون قد يؤدي إلى تفسيرات واسعة تستخدم لتقييد الحريات الفردية.
8. **تقييد حرية الإبداع:** قد يؤثر القانون سلباً على حرية الإبداع الفني والأدبي والعلمي عبر الإنترنت.
9. **الحد من التبادل الثقافي والعلمي:** قد يؤدي تطبيق القانون بشكل صارم إلى الحد من التبادل الثقافي والعلمي عبر الإنترنت مع المجتمع الدولي.

هذه المخاطر دفعت منظمات حقوقية إلى المطالبة بإلغاء القانون أو تعديله لضمان حماية الحقوق الأساسية والحريات الفردية في ليبيا.

الفصل الثالث
إلغاء القانون رقم 5 لسنة 2022

دعت منظمات حقوقية إلى إلغاء القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا أو تعديله لضمان حماية الحقوق الأساسية والحريات الفردية. وفيما يلي النقاط الرئيسية:

1. طالبت مجموعة من المنظمات الحقوقية مجلس النواب الليبي بإلغاء القانون رقم 5 لسنة 2022 الصادر في 27 سبتمبر 2022.
2. دعت هذه المنظمات السلطات الليبية إلى عدم تطبيق القانون بسبب مساسه المباشر بحقوق الإنسان والحريات الأساسية.
3. أشارت المنظمات إلى أن القانون يؤثر سلباً على الحق في حرية التعبير والرأي، والحق في حرية التجمع السلمي، بالإضافة إلى الحق في الخصوصية وحماية المعطيات الشخصية.
4. انتقدت المنظمات القانون لأنه يقنن الرقابة الشاملة للسلطة التنفيذية على الفضاء الرقمي دون إذن قضائي، مع إمكانية حجب المواقع والمحتوى.
5. أشارت المنظمات إلى غياب مبدأ الحوار والتشارك مع مختلف الفاعلين وأصحاب المصلحة عند صياغة القانون.

هذه المطالبات تعكس المخاوف الجدية من تأثير القانون على الحريات الفردية وحقوق الإنسان في ليبيا، وندعو إلى ضرورة مراجعته أو إلغائه لضمان توافقه مع المعايير الدولية لحقوق الإنسان.

المطالب التي يقدمها المجتمع المدني لإلغاء القانون رقم 5 لسنة 2022

قدم المجتمع المدني والمنظمات الحقوقية المطالب التالية بشأن القانون رقم 5 لسنة 2022:

1. إلغاء القانون: طالبت المنظمات مجلس النواب الليبي بإلغاء القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية الصادر في 27 سبتمبر 2022.
2. عدم تطبيق القانون: دعت المنظمات الدولية السلطات الليبية إلى عدم تطبيق القانون بسبب مساسه المباشر بحقوق الإنسان والحريات الأساسية.
3. حماية الحقوق الأساسية: وأشارت المنظمات إلى أن القانون يؤثر سلبا على:
   - الحق في حرية التعبير والرأي
   - الحق في حرية التجمع السلمي
   - الحق في الخصوصية وحماية المعطيات الشخصية

4. منع الرقابة الشاملة: انتقدت المنظمات القانون لأنه يقنن الرقابة الشاملة للسلطة التنفيذية على الفضاء الرقمي دون إذن قضائي، مع إمكانية حجب المواقع والمحتوى.
5. ضمان الحوار والتشارك: وأشارت المنظمات إلى غياب مبدأ الحوار والتشارك مع مختلف الفاعلين وأصحاب المصلحة عند صياغة القانون.

هذه المطالب تعكس مخاوف المجتمع المدني من تأثير القانون على الحريات الفردية وحقوق الإنسان في ليبيا، ودعوتهم لمراجعة القانون أو إلغائه لضمان توافقه مع المعايير الدولية لحقوق الإنسان.

كيف يمكن تصحيح وتحسين القانون رقم 5 لسنة 2022

لتصحيح وتحسين القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الإلكترونية في ليبيا، يمكن اقتراح التعديلات التالية:

1. تحديد نطاق صلاحيات الهيئة الوطنية لأمن وسلامة المعلومات بشكل أكثر دقة، لضمان عدم التعدي على الحريات الشخصية وحرية التعبير.
2. إضافة ضمانات قانونية لحماية خصوصية المستخدمين وبياناتهم الشخصية.
3. توضيح المصطلحات الغامضة مثل "المساس بأمن المجتمع واستقراره" لتجنب التفسيرات الواسعة التي قد تقيد حرية التعبير.
4. إدراج استثناءات واضحة لحماية الصحفيين والمدافعين عن حقوق الإنسان من الملاحقة القانونية عند ممارسة عملهم المشروع.
5. تعزيز الضمانات القضائية، مثل ضرورة الحصول على إذن قضائي قبل مراقبة أو حجب المحتوى الإلكتروني.
6. إضافة بنود تتعلق بالتوعية والتثقيف حول الأمن السيبراني والاستخدام الآمن للإنترنت.
7. مراجعة العقوبات لضمان تناسبها مع طبيعة الجرائم، مع التركيز على الإصلاح والردع بدلاً من العقاب الشديد فقط.
8. إنشاء آلية مستقلة لمراقبة تطبيق القانون وضمان عدم إساءة استخدامه.

هذه التعديلات يمكن أن تساعد في تحقيق توازن أفضل بين مكافحة الجرائم الإلكترونية وحماية الحقوق والحريات الأساسية.

الباب الرابع
الفصل الأول

أنواع الجرائم الإلكترونية

الجرائم الإلكترونية هي أفعال ضارة ترتكب باستخدام التكنولوجيا الحديثة ووسائل الاتصال بالإنترنت والحواسيب. وتنقسم إلى عدة أنواع رئيسية:

جرائم الاختراق والدخول غير المشروع: اختراق الأنظمة والحسابات الشخصية بهدف سرقة المعلومات أو إلحاق الضرر.

1. **جرائم التزوير والاحتيال الإلكتروني**: مثل انتحال الشخصيات وعمليات الاحتيال المالي عبر الإنترنت.
2. **جرائم المساس بالخصوصية**: كالتجسس الإلكتروني وانتهاك خصوصية البيانات الشخصية.
3. **جرائم الإرهاب الإلكتروني**: استخدام الإنترنت لنشر الأفكار المتطرفة وتجنيد الإرهابيين.
4. **جرائم الابتزاز الإلكتروني**: تهديد الضحايا ومساومتهم للحصول على مكاسب مادية.
5. **جرائم القرصنة:** سرقة الملكية الفكرية والبرمجيات.
6. **جرائم غسيل الأموال الإلكتروني**

تتميز هذه الجرائم بإمكانية ارتكابها عن بعد دون تواجد الجاني في مكان الحدث، مما يجعلها أكثر خطورة وصعوبة في المكافحة.

جرائم ضد الأفراد

- سرقة الهوية الشخصية والمعلومات الخاصة
- الاحتيال والنصب عبر البريد الإلكتروني والإنترنت
- المطاردة الإلكترونية والتحرش

جرائم ضد المؤسسات

- اختراق أنظمة المؤسسات وسرقة البيانات الحساسة
- هجمات البرمجيات الخبيثة تعطيل الأنظمة
- التصيد الاحتيالي المستهدف (التصيد بالحربة) خداع موظفي المؤسسة

الفئات المستهدفة الأكثر شيوعاً في الجرائم الإلكترونية :

الفئات الأكثر استهدافاً في الجرائم الإلكترونية هي:

1. النساء والفتيات: يعتبرن من أكثر الفئات تعرضاً للاستهداف، خاصة في جرائم الابتزاز ونشر المحتوى غير الأخلاقي.
2. الشباب: يشكلون فئة مستهدفة بشكل كبير في الجرائم الإلكترونية.
3. الأطفال: يعتبرون من الفئات الضعيفة والمعرضة للاستغلال عبر الإنترنت.
4. الأفراد بشكل عام: يتعرضون لمختلف أنواع الجرائم الإلكترونية مثل سرقة الهويات والمعلومات الشخصية والاحتيال المالي.
5. المؤسسات والشركات: تستهدف بجرائم اختراق الأنظمة وسرقة البيانات الحساسة.

تجدر الإشارة إلى أن هذه الفئات تكون عرضة للاستهداف بسبب عوامل مختلفة مثل ضعف الوعي الأمني، أو قلة الخبرة في التعامل مع التكنولوجيا، أو حساسية المعلومات التي يمتلكونها.

أنواع الجرائم الإلكترونية التي تؤثر على الأفراد بشكل مباشر:

الجرائم الإلكترونية التي تؤثر على الأفراد بشكل مباشر تشمل:

1. **سرقة الهوية:** انتحال شخصية الضحية واستخدام معلوماتها الشخصية بشكل غير قانوني.
2. **الاحتيال على بطاقات الائتمان**: سرقة بيانات البطاقات الائتمانية واستخدامها في عمليات شراء غير مصرح بها.
3. **الابتزاز الإلكتروني**: تهديد الضحايا ومساومتهم للحصول على مكاسب مادية أو معنوية.
4. **المضايقات والإزعاج الإلكتروني**: إرسال رسائل مزعجة أو تهديدات عبر وسائل التواصل الإلكترونية.
5. **نشر المحتوى غير الأخلاقي**: نشر صور أو فيديوهات خاصة بالضحية دون إذنها.
6. **سرقة البريد الإلكتروني**: اختراق حسابات البريد الإلكتروني والوصول إلى المعلومات الشخصية.
7. **التصيد الاحتيالي:** إرسال رسائل خادعة لسرقة المعلومات الشخصية والمالية للضحايا.

هذه الجرائم تؤثر بشكل مباشر على الأفراد، مسببة أضراراً مادية ونفسية وقد تؤدي إلى فقدان الأموال وانتهاك الخصوصية وتشويه السمعة.

كيف يمكن للفرد تحديد إذا كان قد تعرض لجرائم إلكترونية

يمكن للفرد تحديد ما إذا كان قد تعرض لجرائم إلكترونية من خلال مراقبة العلامات التالية:

1. ملاحظة نشاط غير معتاد في الحسابات البنكية أو بطاقات الائتمان، مثل معاملات لم يقم بها.
2. تلقي رسائل تأكيد لعمليات شراء أو تسجيل دخول لم يقم بها.
3. عدم القدرة على الوصول إلى حسابات البريد الإلكتروني أو وسائل التواصل الاجتماعي بسبب تغيير كلمات المرور.
4. ظهور برامج أو تطبيقات غريبة على الأجهزة الإلكترونية.
5. تلقي رسائل تهديد أو ابتزاز عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي.
6. اكتشاف نشر معلومات شخصية أو صور خاصة دون إذن.
7. ملاحظة بطء غير معتاد في أداء الأجهزة الإلكترونية، مما قد يشير إلى وجود برمجيات خبيثة.
8. تلقي إشعارات من مواقع أو خدمات تفيد بحدوث اختراق لقواعد بياناتها.
9. انتحال الشخصية عبر مواقع التواصل الاجتماعي

في حال ملاحظة أي من هذه العلامات، ينبغي على الفرد اتخاذ إجراءات فورية لتأمين حساباته وأجهزته، وإبلاغ السلطات المختصة إذا لزم الأمر.

الخطوات الأولية التي يجب اتخاذها بعد تعرض الفرد لجرائم إلكترونية

إذا تعرض الفرد لجريمة إلكترونية، يجب اتخاذ الخطوات الأولية التالية:

1. **وقف التواصل مع المهاجم:** تجنب الرد على المبتز أو المهاجم.
2. **تأمين الحسابات:** تغيير كلمات المرور لجميع الحسابات المتأثرة وتفعيل المصادقة الثنائية.
3. **إبلاغ السلطات:** تقديم بلاغ للجهات المختصة مثل الشرطة أو وحدة مكافحة الجرائم الإلكترونية.
4. **إبلاغ مزودي الخدمة:** التواصل مع مزودي الخدمة (مثل البنوك أو منصات التواصل الاجتماعي) لإبلاغهم بالحادثة واتخاذ الإجراءات اللازمة.
5. **جمع الأدلة:** الاحتفاظ بنسخ من الرسائل أو أي دليل يمكن أن يساعد في التحقيق.
6. **طلب المساعدة:** التوجه إلى شخص موثوق أو جهة متخصصة للحصول على الدعم والمشورة.

الفصل الثاني

الحماية والوقاية

يمكن للفرد اتخاذ عدة خطوات مهمة لحماية نفسه من الجرائم الإلكترونية في المستقبل. إليك بعض النصائح الأساسية:

1. استخدام برنامج أمان إنترنت شامل:

قم بتثبيت برنامج أمان موثوق مثل Norton 360 لحماية أجهزتك و خصوصيتك عبر الإنترنت وهويتك الرقمية

2. استخدام كلمات مرور قوية:

- استخدم كلمات مرور معقدة تتكون من 12 حرفا على الأقل وتحتوي على مزيج من الأحرف والأرقام والرموز.
- تجنب استخدام نفس كلمة المرور لحسابات مختلفة.
- قم بتغيير كلمات المرور بانتظام.
- استخدم تطبيق إدارة كلمات المرور لتخزين كلمات المرور بشكل آمن

3. تحديث البرامج بإستمرار:

قم بتحديث نظام التشغيل وبرامج الحماية والتطبيقات بانتظام لسد الثغرات الأمنية التي قد يستغلها المجرمون.

- إدارة إعدادات وسائل التواصل الاجتماعي:
- قم بتقييد المعلومات الشخصية التي تشاركها علناً.
- استخدم إعدادات الخصوصية المشددة.
- تجنب نشر تفاصيل حساسة مثل تواريخ السفر أو المعلومات المالية.

4. إدارة إعدادات وسائل التواصل الاجتماعي:

- قم بتقييد المعلومات الشخصية التي تشاركها علنا.
- استخدم إعدادات الخصوصية المشددة.
- تجنب نشر تفاصيل حساسة مثل تواريخ السفر أو المعلومات المالية.

5. تقوية شبكة المنزل:

استخدم كلمة مرور تشفير قوية لشبكة الواي فاي المنزلية.

استخدام شبكة افتراضية خاصة (VPN) تشفير حركة المرور على الإنترنت، خاصة عند استخدام شبكات الواي فاي العامة

6. توعية الأطفال حول سلامة الإنترنت:

علّم أطفالك كيفية استخدام الإنترنت بأمان وشجعهم على إخبارك إذا واجهوا أي مضايقات أو تنمر عبر الإنترنت.

7.البقاء على اطلاع بشأن خروقات الأمان:

تابع الأخبار المتعلقة بـ خروقات البيانات الكبيرة وقم بتغيير كلمات المرور فورا إذا تأثر أي من حساباتك.

8. حماية الهوية الشخصية:

- كن حذرا عند مشاركة المعلومات الشخصية عبر الإنترنت.
- راقب حساباتك بانتظام بحثا عن أي نشاط مشبوه.
- استخدم VPN لحماية أنشطتك عبر الإنترنت، خاصة عند استخدام شبكات الواي فاي العامة.

9. تأمين الأجهزة المحمولة:

- قم بتثبيت برنامج مكافحة الفيروسات.
- استخدم كلمة مرور أو بصمة إصبع لفتح الجهاز.
- قم بتعطيل الاتصال التلقائي بالشبكات وإخفاء البلوتوث عند عدم استخدامه.

10.معرفة كيفية التصرف في حالة وقوع ضحية:

إذا اشتبهت في أنك ضحية لجريمة إلكترونية، أبلغ الشرطة المحلية والسلطات المختصة على الفور واتخاذ الإجراءات اللازمة لحماية حساباتك.

باتباع هذه النصائح، يمكنك تقليل مخاطر الوقوع ضحية للجرائم الإلكترونية بشكل كبير وحماية نفسك وعائلتك ومعلوماتك الشخصية عبر الإنترنت.

الفصل الثالث

الجريمة الإلكترونية والجريمة المعلوماتية

الجرائم المعلوماتية والجرائم الإلكترونية مصطلحان متداخلان لكن هناك فروق بينهما:

الجرائم المعلوماتية تركز على البيانات والبرامج الحاسوبية كعنصر أساسي في ارتكاب الجريمة.

وتنقسم إلى نوعين: جرائم تقع بواسطة النظام المعلوماتي (مثل الاختراق غير المصرح به)، وجرائم تقع على النظام المعلوماتي نفسه.

أما الجرائم الإلكترونية فهي أوسع نطاقاً، وتشمل أي جريمة ترتكب باستخدام وسائل الاتصال الحديثة والحواسيب. هدفها عادة ابتزاز الأشخاص أو تشويه السمعة أو إلحاق الضرر للحصول على مكاسب مادية أو تحقيق أهداف سياسية.

الجرائم الإلكترونية قد تستهدف الأفراد والشركات والمؤسسات الحكومية على حد سواء، وتشكل تهديداً للبنية التحتية الحيوية في مجالات الطاقة والصحة والنقل والخدمات المالية.

أنواع الجرائم المعلوماتية الأكثر شيوعاً تشمل:

1. الاختراق غير المصرح به للأنظمة والحسابات الإلكترونية.
2. سرقة البيانات والمعلومات الشخصية والمالية.
3. الابتزاز الإلكتروني والتهديد عبر الإنترنت.
4. التصيد الاحتيالي عبر رسائل البريد الإلكتروني المزيفة.
5. نشر البرمجيات الخبيثة مثل الفيروسات وأحصنة طروادة.
6. انتحال الشخصية وسرقة الهويات الرقمية.
7. التشهير والتحريض عبر وسائل التواصل الاجتماعي.
8. الاحتيال المالي والنصب الإلكتروني.
9. سرقة الملكية الفكرية والقرصنة.
10. اختراق أنظمة نقاط البيع وسرقة بيانات بطاقات الائتمان.

هذه الجرائم تستهدف الأفراد والشركات والمؤسسات على حد سواء، وتشكل تهديداً متزايداً مع تطور التكنولوجيا وزيادة الاعتماد على الأنظمة الرقمية.

من أبرز حالات الجرائم المعلوماتية التي حدثت مؤخراً:

1. عمليات الاحتيال عبر البريد الإلكتروني والإنترنت، حيث يتم خداع الضحايا للحصول على معلوماتهم الشخصية أو المالية.
2. سرقة البيانات المالية وبطاقات الائتمان من خلال اختراق أنظمة الشركات والمؤسسات.
3. هجمات البرمجيات الخبيثة التي تستهدف إصابة أنظمة الكمبيوتر والشبكات بالفيروسات لسرقة البيانات أو تعطيل الأنظمة.
4. عمليات القرصنة واختراق الحسابات الشخصية والمؤسسية على مواقع التواصل الاجتماعي.
5. التصيد الاحتيالي عبر مواقع وتطبيقات مزيفة لسرقة بيانات تسجيل الدخول والمعلومات الحساسة.
6. الابتزاز الإلكتروني وتهديد الضحايا بنشر معلومات أو صور خاصة.
7. الهجمات السيبرانية على البنى التحتية الحيوية والمؤسسات الحكومية.

هذه الحالات تعكس تطور أساليب المجرمين الإلكترونيين واستغلالهم للتقنيات الحديثة، مما يستدعي تعزيز إجراءات الأمن السيبراني والتوعية بمخاطر هذه الجرائم.

الباب الخامس

الفصل الأول

الجريمة الإلكترونية والجريمة السيبرانية

لا يوجد فرق جوهري بين الجريمة الإلكترونية والجريمة السيبرانية،فهما مصطلحان يشيران إلى نفس النوع من الجرائم:

1. كلا المصطلحين يشيران إلى الجرائم التي ترتكب باستخدام تكنولوجيا المعلومات والاتصالات الحديثة.
2. يستخدم الخبراء مصطلح "الجريمة السيبرانية" (Cybercrime) للإشارة إلى كل من الجرائم الإلكترونية والمعلوماتية.
3. تشمل هذه الجرائم أنشطة مثل الاحتيال الإلكتروني، سرقة الهوية، اختراق الأنظمة، نشر البرمجيات الخبيثة، وغيرها.
4. تستهدف هذه الجرائم الأفراد والمؤسسات والحكومات، وغالباً ما تهدف إلى تحقيق مكاسب مادية أو سياسية.
5. تتميز هذه الجرائم بطابعها المعقد وعابر للحدود، مما يجعل مكافحتها تحدياً يتطلب تعاوناً دولياً.

باختصار، الجريمة الإلكترونية والجريمة السيبرانية هما وجهان لعملة واحدة، و يشيران إلى نفس النوع من الأنشطة الإجرامية التي تتم في الفضاء الرقمي.

أشهر أنواع الجريمة السيبرانية

أبرز أنواع الجرائم السيبرانية الأكثر شيوعاً تشمل:

1. **التصيد الإلكتروني:** محاولات خداع المستخدمين للحصول على معلوماتهم الشخصية والمالية.
2. **برمجيات الفدية:** برامج خبيثة تشفير بيانات الضحية وتطالب بفدية لفك التشفير.
3. **الاحتيال الإلكتروني:** عمليات نصب واحتيال تتم عبر الإنترنت.
4. **سرقة الهوية:** الحصول على المعلومات الشخصية للضحايا واستخدامها بشكل غير قانوني.
5. **اختراق الحسابات:** الوصول غير المصرح به لحسابات المستخدمين.

6. **نشر البرمجيات الخبيثة:** مثل الفيروسات وأحصنة طروادة.
7. **الابتزاز الإلكتروني:** تهديد الضحايا بنشر معلومات حساسة عنهم.
8. **انتحال الشخصية:** التظاهر بشخصية شخص آخر لأغراض احتيالية.
9. **الهجمات على المؤسسات والشركات:** استهداف البنية التحتية والبيانات الحساسة للمؤسسات.

تستهدف هذه الجرائم الأفراد والمؤسسات على حد سواء، وتشكل تهديداً كبيراً للأمن السيبراني والخصوصية في العصر الرقمي.

كيف يمكن حماية النظم المعلوماتية من الاختراقات

لحماية النظم المعلوماتية من الاختراقات، يمكن اتباع عدة إجراءات أمنية فعالة:

1. تحديث نظام التشغيل والتطبيقات باستمرار لسد الثغرات الأمنية.
2. استخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة وتحديثها بانتظام.
3. تطبيق كلمات مرور قوية ومعقدة تتكون من 8 أحرف على الأقل وتشمل أرقاماً وأحرفاً كبيرة وصغيرة ورموزاً.
4. تشفير البيانات الحساسة لحمايتها من السرقة والتلاعب.
5. إنشاء نسخ احتياطية منتظمة للبيانات الهامة وتخزينها في مواقع آمنة.
6. تثبيت جدار الحماية وبرامج منع الوصول غير المصرح به إلى قواعد البيانات.
7. تدريب الموظفين على أفضل ممارسات الأمن السيبراني وتوعيتهم بمخاطر الاختراق.
8. تطبيق مبدأ الصلاحيات المحدودة بحيث يتم منح الموظفين حق الوصول للبيانات حسب حاجة العمل فقط.
9. استخدام التوثيق متعدد العوامل للتحقق من هوية المستخدمين.
10. إجراء اختبارات اختراق دورية لتحديد نقاط الضعف في النظام ومعالجتها.

بتطبيق هذه الإجراءات مجتمعة، يمكن تعزيز أمن النظم المعلوماتية بشكل كبير وحمايتها من معظم محاولات الاختراق.

ما هي الاستراتيجيات والتقنيات الحديثة لحماية البيانات من الاختراق

هناك عدة استراتيجيات وتقنيات حديثة فعالة لحماية البيانات من الاختراقات:

1. استخدام برامج مكافحة الفيروسات والبرمجيات الخبيثة المتطورة وتحديثها باستمرار.
2. تحديث أنظمة التشغيل والتطبيقات بشكل دوري لسد الثغرات الأمنية.
3. تطبيق كلمات مرور قوية ومعقدة تتكون من 8 أحرف على الأقل وتشمل أرقاماً وأحرفاً كبيرة وصغيرة ورموزاً.
4. تشفير البيانات الحساسة لحمايتها من السرقة والتلاعب.
5. إنشاء نسخ احتياطية منتظمة للبيانات الهامة وتخزينها في مواقع آمنة، بما في ذلك التخزين السحابي.
6. تثبيت جدار الحماية وبرامج منع الوصول غير المصرح به إلى قواعد البيانات.
7. تطبيق مبدأ الصلاحيات المحدودة بحيث يتم منح الموظفين حق الوصول للبيانات حسب حاجة العمل فقط.
8. استخدام التوثيق متعدد العوامل للتحقق من هوية المستخدمين.
9. إجراء اختبارات اختراق دورية لتحديد نقاط الضعف في النظام ومعالجتها.
10. تدريب الموظفين على أفضل ممارسات الأمن السيبراني وتوعيتهم بمخاطر الاختراق.

بتطبيق هذه الاستراتيجيات والتقنيات مجتمعة، يمكن تعزيز أمن البيانات بشكل كبير وحمايتها من معظم محاولات الاختراق.

الفصل الثاني

جريمة الابتزاز الإلكتروني

الابتزاز الإلكتروني هو شكل من أشكال التهديد والترهيب عبر الإنترنت، حيث يقوم المبتز بتهديد الضحية بنشر صور أو مقاطع فيديو أو معلومات سرية خاصة بها، مقابل الحصول على مبالغ مالية أو منافع أخرى.

عادة ما تبدأ عملية الابتزاز بإقامة علاقة صداقة مع الضحية عبر وسائل التواصل الاجتماعي، ثم استدراجها للتواصل عبر برامج المحادثات المرئية، حيث يتم تسجيل محتوى مسيء للضحية واستخدامه لابتزازها لاحقاً.

يمكن أن يحدث الابتزاز أيضاً عندما يرسل الأشخاص صورهم الخاصة طواعية لآخرين، كالأصدقاء أو الشركاء، الذين يسيئون استخدامها لاحقاً.

للحماية من الابتزاز الإلكتروني، ينصح بتوخي الحذر عند التعامل مع الغرباء عبر الإنترنت، وعدم مشاركة معلومات أو صور خاصة، واستخدام إعدادات الخصوصية على مواقع التواصل الاجتماعي.

في حال التعرض للابتزاز، يجب عدم الاستجابة لمطالب المبتز والإبلاغ عن الحادث للسلطات المختصة فوراً.

الخطوات الأولى التي يجب اتخاذها عند تعرضك لابتزاز إلكتروني؟

إذا تعرضت لابتزاز إلكتروني، فإليك الخطوات الأولى التي يجب اتخاذها:

1. لا تتواصل مع المبتز أو تستجيب لمطالبه. قطع الاتصال معه هو الخطوة الأولى الهامة.
2. احتفظ بجميع الأدلة كالرسائل والصور وسجلات المكالمات. وثق كل شيء يتعلق بالابتزاز.
3. تواصل مع شخص موثوق به كأحد أفراد العائلة أو صديق مقرب للحصول على الدعم النفسي والمشورة.
4. لا تصدق تهديدات المبتز أو وعوده. غالباً ما يكون المبتز خائفاً ويحاول استغلال ضعفك.
5. تواصل مع الجهات الأمنية المختصة بمكافحة الجرائم الإلكترونية وأبلغهم عن الحادثة. هذا هو الحل الأمثل والنهائي للمشكلة.
6. حافظ على هدوئك وقوتك. ردة فعلك القوية والمتزنة في البداية ستحدد مسار القضية وقد تردع المبتز.

تذكر أن عدم الاستجابة لمطالب المبتز والتوجه للجهات المختصة هو أفضل طريقة للتعامل مع هذا الموقف.

الخدمات المتخصصة في مكافحة الابتزاز الإلكتروني

هناك عدة خدمات متخصصة في مكافحة الابتزاز الإلكتروني، تشمل:

1. خدمات قانونية: تقدم المشورة القانونية واتخاذ الإجراءات القانونية ضد المبتزين من خلال محامين متخصصين.
2. خدمات تقنية: تساعد في حل المشاكل التقنية وتوفر الدعم الفني اللازم للتعامل مع قضايا الابتزاز الإلكتروني.
3. خدمات نفسية وإرشادية: تقدم الدعم النفسي والتوجيه للضحايا لمساعدتهم على تجاوز الأزمة.
4. خدمات حذف المحتوى: تعمل على إزالة المحتوى الضار أو الفاضح من وسائل التواصل الاجتماعي والإنترنت.
5. خدمات التبليغ والشكاوى: تسهل عملية الإبلاغ عن حالات الابتزاز للجهات المختصة.
6. خدمات التوعية والوقاية: تقدم معلومات وإرشادات للوقاية من الابتزاز الإلكتروني.
7. خدمات على مدار الساعة: توفر المساعدة والدعم للضحايا في أي وقت.

هذه الخدمات تهدف إلى مساعدة الضحايا في التعامل مع حالات الابتزاز الإلكتروني بشكل شامل، من النواحي القانونية والتقنية والنفسية.

أفضل الطرق لتحديد هوية المبتز

تحديد هوية المبتز أمر معقد ويجب أن يتم من قبل الجهات الأمنية المختصة. ومع ذلك، هناك بعض الخطوات التي يمكن اتخاذها للمساعدة في هذه العملية:

1. جمع وتوثيق كافة الأدلة المتعلقة بالابتزاز، بما في ذلك الرسائل والصور وسجلات المكالمات.
2. تحليل عناوين البريد الإلكتروني وأرقام الهواتف المستخدمة في الابتزاز، فقد تحتوي على معلومات مفيدة.
3. فحص الحسابات المزيفة على وسائل التواصل الاجتماعي التي قد يستخدمها المبتز للتخفي.

4. مراجعة سجلات الاتصالات وبيانات الإنترنت للبحث عن أنماط أو معلومات قد تساعد في تحديد الهوية.
5. الاستعانة بخبراء الأمن السيبراني لتتبع الأنشطة الإلكترونية للمبتز.
6. التعاون مع الشرطة والجهات الأمنية المختصة، فلديهم الأدوات والصلاحيات اللازمة لإجراء تحقيق شامل.

من المهم عدم محاولة تحديد هوية المبتز بنفسك، حيث قد يؤدي ذلك إلى تعريض سلامتك للخطر أو إتلاف الأدلة. بدلاً من ذلك، قم بإبلاغ السلطات المختصة فوراً وتزويدهم بكافة المعلومات المتاحة.

الحماية من الابتزاز الالكتروني

لحماية نفسك من الابتزاز الإلكتروني، اتبع الخطوات التالية:

1. تعامل بحذر شديد مع الغرباء على وسائل التواصل الاجتماعي ولا تمنح ثقتك بسرعة للآخرين.
2. لا تشارك معلومات شخصية أو صور خاصة مع أشخاص غير معروفين.
3. استخدم كلمات مرور قوية وفريدة لكل حساب، وقم بتحديثها بانتظام.
4. فعّل خاصية المصادقة الثنائية على جميع حساباتك الإلكترونية.
5. راجع إعدادات الخصوصية والأمان لحساباتك على وسائل التواصل الاجتماعي بشكل دوري.
6. كن حذراً عند فتح روابط أو مرفقات من مصادر غير موثوقة.
7. حافظ على تحديث برامج مكافحة الفيروسات وجدران الحماية على أجهزتك.
8. قم بتوعية أفراد عائلتك، خاصة الأطفال والمراهقين، حول مخاطر الابتزاز الإلكتروني وكيفية تجنبه.
9. في حال تعرضك للابتزاز، لا تستجب لمطالب المبتز وتوقف عن مراسلته فوراً.
10. أبلغ الجهات المختصة فوراً إذا تعرضت لأي محاولة ابتزاز.

تذكر أن الوقاية خير من العلاج، لذا كن يقظاً دائماً عند استخدام الإنترنت ووسائل التواصل الاجتماعي.

كيف يمكنني معرفة إذا كنت مؤهلاً للحصول على المساعدة القانونية :

لمعرفة ما إذا كنت مؤهلاً للحصول على المساعدة القانونية في حالات الابتزاز الإلكتروني، يمكنك اتباع الخطوات التالية:

1. تواصل مع الجهات الأمنية المختصة بمكافحة الجرائم الإلكترونية وقدم لهم تفاصيل حالتك. سيقومون بتقييم الموقف وإرشادك إلى الخيارات القانونية المتاحة.
2. استشر محامياً متخصصاً في الجرائم الإلكترونية. معظم المحامين يقدمون استشارات أولية مجانية أو بتكلفة منخفضة لتقييم قضيتك.
3. ابحث عن منظمات غير حكومية أو جمعيات متخصصة في مكافحة الجرائم الإلكترونية. غالباً ما تقدم هذه الجهات مساعدة قانونية مجانية أو بتكلفة مخفضة للضحايا.
4. قم بتوثيق جميع الأدلة المتعلقة بالابتزاز، مثل الرسائل والصور ولقطات الشاشة. كلما كانت الأدلة أقوى، زادت فرصتك في الحصول على المساعدة القانونية.
5. تحقق من وجود برامج مساعدة قانونية حكومية في منطقتك مخصصة لضحايا الجرائم الإلكترونية.

تذكر أن معظم الحالات الجادة من الابتزاز الإلكتروني تستحق المساعدة القانونية، لذا لا تتردد في طلب المشورة والدعم.

جريمة التشهير الالكتروني

التشهير الإلكتروني يتم فيه إذلال وفضح الأشخاص علناً بسبب أفعالهم التي تمت في الخفاء أو دون رغبتهم في نشرها. يتضمن نشر معلومات خاصة على الإنترنت، مما قد يؤدي إلى رسائل كراهية وتهديدات.

هناك عدة أنواع للتشهير الإلكتروني، منها:

1. التشهير الحكومي: تستخدمه الحكومات كعقوبة للتهرب الضريبي والانتهاكات البيئية والجرائم البسيطة.
2. التشهير التنظيمي: تقوم به الهيئات الإدارية لنشر معلومات سلبية عن الشركات الخاضعة للرقابة.

يعتبر التشهير الإلكتروني جريمة في العديد من الدول. في الجزائر، على سبيل المثال، هناك إشكاليات حول توحيد المفهوم وضبط المعايير القانونية المتعلقة به في الفضاء السيبراني.

في المملكة العربية السعودية، يعاقب القانون على التشهير بالآخرين عبر وسائل تقنيات المعلومات بالسجن لمدة لا تزيد على ثلاث سنوات وغرامة مالية.

كيف يؤثر التشهير الإلكتروني على حياة الأفراد والمجتمعات:

التشهير الإلكتروني يؤثر بشكل كبير وسلبي على حياة الأفراد والمجتمعات:

1. يؤدي إلى اغتيال معنوي للأشخاص المستهدفين من خلال نشر معلومات خاصة أو مسيئة عنهم.
2. يسبب أضراراً نفسية واجتماعية للضحايا، حيث يفقدهم احترامهم وتقديرهم في محيطهم.
3. قد يؤدي إلى تهديدات بالقتل ورسائل كراهية تجاه الضحايا، مما يعرض سلامتهم للخطر.
4. يمكن أن يدمر حياة الضحايا بالكامل، حيث يتعرضون للترصد والمراقبة الإلكترونية والإيذاء البدني والنفسي.
5. يواجه الضحايا صعوبات في العمل وقد يفقدون وظائفهم نتيجة التشهير.
6. يهدد استقرار المجتمعات من خلال نشر الفوضى والكراهية.
7. يقوض الثقة بين أفراد المجتمع ويشجع على انتهاك الخصوصية.
8. قد يؤدي إلى الابتزاز و الإكراه والمضايقة والتنمر.

لذا فإن التشهير الإلكتروني له آثار مدمرة على الأفراد نفسياً واجتماعياً ومهنياً، كما أنه يهدد تماسك النسيج الاجتماعي ويشيع أجواء من عدم الثقة والخوف في المجتمع.

ما هي أبرز حالات التشهير التي شهدها العالم

أبرز حالات التشهير التي شهدها العالم تشمل:

1. **فضيحة "ساكو"**: حيث تم نشر معلومات كاذبة على تويتر، مما أثار جدلاً حول دور وسائل الإعلام في التحقق من المعلومات قبل نشرها.
2. **التشهير عبر مواقع التواصل الاجتماعي:** انتشار ظاهرة التشهير الإلكتروني، حيث يتم نشر معلومات خاصة أو صور بهدف تشويه سمعة الأفراد، مما يؤدي إلى رسائل كراهية وتهديدات بالقتل.
3. **التشهير الحكومي**: مثلما تقوم إدارة الغذاء والدواء الأمريكية بالتشهير بالشركات التي تعرقل المنافسة في صناعة الأدوية.

أسباب انتشار التشهير على الإنترنت

انتشار التشهير على الإنترنت يعود لعدة أسباب رئيسية:

1. **سهولة نشر المعلومات:** الإنترنت يوفر منصة سهلة وسريعة لنشر المحتوى والوصول إلى جمهور واسع بسرعة كبيرة.
2. **صعوبة التحقق من المعلومات:** انتشار الأخبار والمعلومات بسرعة يجعل من الصعب التحقق من صحتها قبل انتشارها على نطاق واسع.
3. **الانفتاح الرقمي:** زيادة مشاركة الناس لحياتهم الخاصة على وسائل التواصل الاجتماعي يجعلهم أكثر عرضة للتشهير.
4. **ضعف الوعي بالخصوصية:** كثير من الناس لا يدركون مخاطر مشاركة معلوماتهم الشخصية عبر الإنترنت.
5. **سهولة إخفاء الهوية:** إمكانية النشر بأسماء مستعارة تشجع البعض على التشهير دون خوف من العواقب.
6. **تغير القيم المجتمعية**: ميل المجتمع للفضح أكثر من الستر، وانتشار ثقافة كشف الخصوصيات.
7. **ضعف الرقابة والعقوبات**: صعوبة تتبع وملاحقة مرتكبي التشهير الإلكتروني قانونياً في كثير من الحالات.

الفصل الثالث

انتحال الشخصية الالكتروني

انتحال الشخصية الإلكتروني، المعروف بأسم "الانتحال الإلكتروني" أو "catfishing"، هو شكل من أشكال الخداع عبر الإنترنت يتضمن إنشاء هوية مزيفة أو شخصية وهمية على مواقع التواصل الاجتماعي أو المنصات الإلكترونية الأخرى.

الأشخاص الذين يمارسون الانتحال الإلكتروني عادة ما يستخدمون صوراً وحقائق حقيقية لشخص آخر لجعل الهوية المزيفة تبدو واقعية. غالباً ما يكون الشخص الحقيقي الذي تُستخدم هويته غير مدرك لذلك.

هناك عدة دوافع وراء الانتحال الإلكتروني، منها:

- إنشاء علاقات رومانسية وهمية عبر الإنترنت
- ارتكاب عمليات احتيال مالي
- التنمر الإلكتروني
- استدراج الضحايا للقاء شخصي بهدف الإيذاء أو الاختطاف

يشكل الانتحال الإلكتروني مخاطر عديدة، خاصة عندما يُستخدم لأستدراج الأشخاص إلى مواقف خطرة أو للتحرش الجنسي.

للحماية من الانتحال الألكتروني، يُنصح باتباع بعض الإجراءات الوقائية:

- التحقق من هوية الأشخاص عبر الإنترنت قبل تطوير علاقات عميقة معهم.
- عدم مشاركة المعلومات الشخصية الحساسة مع الغرباء عبر الإنترنت.
- توخي الحذر من الرسائل أو الطلبات المشبوهة.
- استخدام إعدادات الخصوصية على مواقع التواصل الاجتماعي.

في العديد من البلدان، يعتبر الانتحال الإلكتروني جريمة يعاقب عليها القانون، خاصة إذا تم استخدامه لارتكاب جرائم أخرى مثل الاحتيال أو الابتزاز.

هناك عدة قواعد أساسية يمكن اتباعها لتحديد الهويات المزورة على الإنترنت:

1. التحقق من الصور: ابحث عن علامات التلاعب بالصور أو استخدام صور شخص آخر عبر البحث العكسي للصور.

2. فحص تاريخ الحساب: الحسابات الجديدة أو التي لديها نشاط محدود قد تكون مشبوهة.

3. تدقيق المعلومات الشخصية: ابحث عن تناقضات في التفاصيل الشخصية المقدمة عبر منصات مختلفة.

4. مراقبة نمط اللغة: الأخطاء اللغوية المتكررة أو استخدام لغة غير متسقة قد يشير إلى هوية مزيفة.

5. الحذر من الطلبات المالية: كن متيقظاً لأي طلبات للمال أو المعلومات المالية الحساسة.

6. التحقق من الروابط: تجنب النقر على روابط مشبوهة قد تؤدي إلى مواقع احتيالية.

7. استخدام المصادقة الثنائية: تفعيل هذه الخاصية على حساباتك لزيادة الأمان.

8. الشك في العروض المغرية جداً: احذر من العروض التي تبدو جيدة بشكل غير واقعي.

9. التواصل خارج المنصة الأصلية: حاول التحقق من هوية الشخص عبر وسائل اتصال أخرى.

10. الثقة في حدسك: إذا شعرت أن شيئاً ما غير طبيعي، فمن الأفضل توخي الحذر والتحقق أكثر.

باتباع هذه القواعد، يمكنك تقليل مخاطر الوقوع ضحية للهويات المزورة على الإنترنت وحماية نفسك من الاحتيال الإلكتروني.

تاريخ الانتحال الإلكتروني:

الانتحال الإلكتروني هو نوع من الخداع الذي يتضمن إنشاء هوية مزيفة على الإنترنت بهدف خداع الآخرين. يعود تاريخ هذا النوع من الاحتيال إلى بدايات استخدام الإنترنت، حيث استغل المحتالون ضعف البنية التحتية الأمنية للبريد الإلكتروني والشبكات الاجتماعية لتحقيق مكاسب شخصية أو مالية.

تطور الانتحال الإلكتروني:

- **البدايات**

في البداية، كان الانتحال الإلكتروني بسيطاً نسبياً، حيث كان يعتمد بشكل أساسي على إنشاء حسابات بريد إلكتروني مزيفة أو استخدام أسماء مزيفة على المنتديات والمواقع الإلكترونية. كان الهدف الأساسي هو خداع الأفراد للحصول على معلومات شخصية أو مالية.

- **تطور التكنولوجيا**

مع تطور التكنولوجيا، أصبح الانتحال الإلكتروني أكثر تعقيداً. على سبيل المثال، أصبح من الممكن انتحال هوية شخص آخر باستخدام صور ومعلومات حقيقية مسروقة من الإنترنت. كما تطورت أساليب الاحتيال لتشمل استخدام الذكاء الاصطناعي لإنشاء شخصيات وهمية تبدو واقعية للغاية، مما يزيد من صعوبة اكتشاف الخداع.

- **البريد الإلكتروني**

من الأشكال الشائعة للانتحال الإلكتروني هو انتحال البريد الإلكتروني، حيث يقوم المحتالون بإنشاء رسائل بريدية تبدو وكأنها مرسلة من مصادر موثوقة. يعود ذلك إلى ضعف بروتوكولات البريد الإلكتروني القديمة التي لا تحتوي على آليات للتحقق من هوية المرسل.

- **وسائل التواصل الاجتماعي**

استغل المحتالون أيضاً منصات التواصل الاجتماعي لإنشاء حسابات مزيفة تهدف إلى خداع المستخدمين. يمكن استخدام هذه الحسابات المزيفة في التنمر الإلكتروني أو استدراج الضحايا إلى مواقف خطرة.

- **الأساليب الشائعة**

1. **انتحال الشخصيات:** إنشاء حسابات مزيفة باستخدام صور ومعلومات مسروقة.
2. **التصيد الاحتيالي:** إرسال رسائل بريد إلكتروني مزيفة للحصول على معلومات حساسة.
3. **الهندسة الاجتماعية:** التلاعب النفسي بالضحايا لدفعهم إلى اتخاذ قرارات غير حكيمة.
4. **استخدام الذكاء الاصطناعي:** إنشاء شخصيات وهمية تبدو واقعية للغاية لخداع الضحايا في تطبيقات المواعدة وغيرها.

- **المخاطر**

تتضمن المخاطر المرتبطة بالانتحال الإلكتروني سرقة الهوية، الاحتيال المالي، التنمر الإلكتروني، وحتى الاستدراج إلى مواقف خطيرة مثل الاختطاف أو الاعتداء.

باختصار، الانتحال الإلكتروني هو تهديد متزايد يتطور مع تطور التكنولوجيا، مما يتطلب من المستخدمين توخي الحذر واتخاذ إجراءات وقائية لحماية أنفسهم.

الطرق الشائعة التي يستخدمها المخادعون الإلكترونيون لتحقيق أهدافهم

يستخدم المخادعون الإلكترونيون عدة طرق شائعة لتحقيق أهدافهم غير المشروعة:

1. **انتحال شخصيات وهمية:** إنشاء حسابات مزيفة على مواقع التواصل الاجتماعي باستخدام صور وتفاصيل شخصية مسروقة لكسب ثقة الضحايا.
2. **الاستدراج العاطفي:** بناء علاقات عاطفية وهمية عبر الإنترنت للتلاعب بمشاعر الضحايا واستغلالهم مالياً أو عاطفياً.
3. **عروض مغرية كاذبة:** تقديم فرص عمل أو استثمار وهمية تبدو جذابة للغاية لاستدراج الضحايا.
4. **التصيد الاحتيالي:** إرسال رسائل إلكترونية أو روابط مزيفة لسرقة المعلومات الشخصية والمالية.
5. **التلاعب النفسي:** استخدام تقنيات الضغط والإلحاح لدفع الضحايا لاتخاذ قرارات متسرعة.
6. **استغلال الثغرات الأمنية:** اختراق الحسابات الشخصية للحصول على معلومات حساسة.
7. **الابتزاز الإلكتروني:** تهديد الضحايا بنشر معلومات أو صور خاصة للحصول على المال أو مزايا أخرى.
8. **التظاهر بتمثيل جهات رسمية:** ادعاء الانتماء لمؤسسات حكومية أو شركات معروفة لخداع الضحايا.
9. **استغلال الأحداث الجارية:** استخدام الأخبار والأزمات الحالية لخلق مخططات احتيالية مرتبطة بها.

10. **المسابقات والجوائز الوهمية:** إغراء الضحايا بجوائز كبيرة مقابل تقديم معلومات شخصية أو دفع رسوم.

لحماية نفسك من هذه الأساليب، من المهم التحقق دائماً من هوية الأشخاص عبر الإنترنت، وتوخى الحذر من العروض المشبوهة، وعدم مشاركة المعلومات الشخصية الحساسة مع الغرباء.

الأدوات التي يمكن استخدامها لمراقبة نشاطات المخادعين الإلكترونيين

هناك عدة أدوات يمكن استخدامها لمراقبة نشاطات المخادعين الإلكترونيين:

1. **برمجيات الرقابة الأبوية:** تساعد في مراقبة نشاط الأطفال على الإنترنت من خلال تصفية المحتوى، حجب المواد غير المناسبة، ومراقبة التطبيقات المستخدمة.
2. **أدوات مراقبة النشاطات وتسجيلات الأحداث:** تستخدم للكشف عن الأنشطة غير المصرح بها أو المشتبه بها على الشبكة أو الأنظمة.
3. **برامج مراقبة الرسائل النصية:** تسمح بمراقبة المحادثات ووضع قيود على جهات الاتصال لحماية الأطفال من التعرض للمضايقة أو التنمر.
4. **أدوات تتبع البحث:** تساعد في التعرف على العبارات والكلمات التي يتم البحث عنها والوصول إلى نتائج البحث.
5. **برامج تحليل السلوك:** توفر تقارير تفصيلية حول طبيعة نشاط المستخدمين وما يفعلونه على الإنترنت.
6. **أدوات تحديد الموقع الجغرافي:** تساعد في التعرف على أماكن وجود المستخدمين لحظة بلحظة.
7. **برامج إدارة الوقت:** تمكن من تعيين حدود زمنية وجدولة أوقات استخدام منصات التواصل الاجتماعي أو مواقع الإنترنت الأخرى.

من المهم ملاحظة أن استخدام هذه الأدوات يجب أن يكون متوافقاً مع القوانين واللوائح المتعلقة بالخصوصية وحماية البيانات. كما يجب استخدامها بمسؤولية وأخلاقية، خاصة عندما يتعلق الأمر بمراقبة الأطفال أو الموظفين.

الباب السادس

الفصل الأول

الهجمات الإلكترونية

الهجمات الإلكترونية هي محاولات ضارة ومتعمدة لاختراق أنظمة المعلومات والشبكات الحاسوبية، وتتضمن عدة أنواع وأساليب منها:

- هجمات التصيد الاحتيالي: تستهدف خداع المستخدمين للحصول على معلومات حساسة
- البرامج الضارة: تشمل الفيروسات وبرامج الفدية التي تخترق الأنظمة عبر استغلال الثغرات الأمنية
- تستخدم شبكات الأجهزة المصاب : هجمات رفض الخدمة الموزعة (روبوت الشبكة) لإرباك الأنظمة وتعطيله
- التجسس الصناعي: يستهدف سرقة المعلومات الحساسة والأسرار التجارية.
- الهجمات على البنية التحتية: تستهدف أنظمة حيوية مثل شبكات الكهرباء والمياه.

<u>وصلت الجرائم الإلكترونية إلى حد القتل</u>؛ ففي شهر 9 من عام 2020، توفيت امرأة ف دوسلدورف في أحد المستشفيات الألمانية بعد تعطل نظام الحاسوب بسبب برنامج للقرصنة بواسطة الفدية، وهو برنامج خبيث يقيد الوصول إلى نظام الحاسوب الذي يصيبه. ويعكس هذا الهجوم الإلكتروني مدى هشاشة القطاع الصحي في مواجهة هذه الهجمات. وقال الكاتب أنوش سيد تاغيا في تقرير نشرته السويسرية، إنه لم يحدث أن سُجلت حالات وفاة نتيجة هجوم (le temps) صحيفة لوتون إلكتروني. ولكن تسبب هجوم سيبراني في وفاة مريضة في مستشفى بدوسلدورف نتيجة عدم تلقيها للعلاج. وأعلنت السلطات الألمانية عن العواقب المأساوية للهجوم السيبراني «الإلكتروني» الذي استهدف الشبكة الإلكترونية للمستشفى الجامعي في دوسلدورف ليصيب أنظمته بالشلل الجزئي منذ 9 سبتمبر/أيلول 1

وبرنامج الفدية المعروف باسم «رانسوم وير» هو برنامج ضار يستهدف نقاط الضعف في برامج معينة للسماح للمهاجمين بالتحكم عن بُعد في أنظمة الحاسوب. ومقابل إعادة الوصول إلى الملفات المحملة على أجهزة الحاسوب عادة ما يطلب المخترق فدية تصل إلى عشرات أو حتى مئات الآلاف من الدينارات

أهم التحديات التي تواجهها الجهات الأمنية في مكافحة الجرائم الالكترونية

تواجه الجهات الأمنية عدة تحديات رئيسية في مكافحة الجرائم الإلكترونية

التطور السريع للتكنولوجيا: يتطلب من السلطات القانونية مواكبة مستمرة لأحدث التطورات التقنية

تعقيد الجرائم الإلكترونية: تتنوع الأساليب والتقنيات المستخدمة، مما يصعب تحديد طرق فعالة لمكافحته

التحديات المتعلقة بالأدلة الرقمية: صعوبة جمع وتقديم الأدلة القانونية اللازمة للإدعاء في القضايا الإلكترونية

التشفير والأمان الرقمي: يعيق الوصول إلى المعلومات المطلوبة للتحقيق

تزايد حجم البيانات: يصعب تحليل وفرز كميات هائلة من البيانات

الفراغ التشريعي: وجود ثغرات في القوانين والتشريعات المتعلقة بالجرائم الإلكترونية

البطء في سن التشريعات: عدم مواكبة القوانين للتطور السريع في أساليب الجرائم الإلكترونية

الحاجة للتعاون الدولي: ضرورة التنسيق مع المنظمات الدولية لتبادل الخبرات ومواجهة الجرائم العابرة للحدود

لمواجهة هذه التحديات، يتطلب الأمر تطوير استراتيجيات متقدمة، تحديث القوانين باستمرار، وتدريب فرق متخصصة في مكافحة الجرائم الإلكترونية

كيف يمكن للتعاون الدولي مساعدة الجهات الأمنية في مكافحة الجرائم الإلكترونية

يمكن للتعاون الدولي مساعدة الجهات الأمنية في مكافحة الجرائم الإلكترونية بعدة طرق مهمة:

1. **تبادل الخبرات والمعلومات:** يساعد التعاون مع المنظمات الدولية مثل الأمم المتحدة والاتحاد الأوروبي في تبادل الخبرات وتطوير استراتيجيات فعالة لمكافحة الجرائم الإلكترونية.
2. **تسريع الإجراءات وتبادل المعلومات:** يساهم التعاون الدولي في تسريع عمليات تبادل المعلومات في القضايا التي تقع في دول مختلفة، مما يسهل التحقيقات.

3. **مواجهة الجرائم العابرة للحدود:** نظراً لأن الجرائم الإلكترونية غالباً ما تكون عابرة للحدود، فإن التعاون الدولي ضروري لمكافحتها بفعالية.
4. **تطوير القوانين والتشريعات:** يساعد التعاون الدولي في تطوير قوانين وتشريعات متناسقة عالمياً لمواجهة الجرائم الإلكترونية.
5. **بناء القدرات:** من خلال برامج تدريبية دولية لتبادل الخبرات مع الدول المتقدمة في مجال مكافحة الجرائم الإلكترونية.
6. **التعامل مع منصات التواصل الاجتماعي:** يمكن للتعاون الدولي أن يساعد في تحسين التعاون مع منصات التواصل الاجتماعي العالمية للحصول على المعلومات اللازمة.
7. **مواجهة تحديات الشبكة الخفية:** التعاون الدولي ضروري لمواجهة تحديات الشبكة الخفية التي تخفي هوية مستخدميها.

هذا التعاون الدولي يعد ضرورياً نظراً للطبيعة العابرة للحدود للجرائم الإلكترونية وسرعة تطورها.

كيف يمكن تطوير قوانين تنظيمية محدثة لمواجهة الجرائم الإلكترونية

لتطوير قوانين تنظيمية محدثة لمواجهة الجرائم الإلكترونية، يمكن اتباع الخطوات التالية:

1. **مراجعة دورية للقوانين:** إجراء مراجعات منتظمة للتشريعات القائمة لضمان مواكبتها للتطورات التكنولوجية والجرائم المستجدة.
2. **التعاون الدولي:** العمل مع المنظمات الدولية مثل الأمم المتحدة والاتحاد الأوروبي لتبادل الخبرات وتطوير استراتيجيات عالمية موحدة.
3. **استشارة الخبراء:** الاستعانة بخبراء في مجال الأمن السيبراني والقانون لصياغة تشريعات فعالة ومتخصصة.
4. **مرونة التشريعات:** صياغة القوانين بطريقة مرنة تسمح بتطبيقها على التقنيات الجديدة دون الحاجة لتعديلات متكررة.
5. **التوازن بين الأمن والحريات:** ضمان أن تحمي القوانين الأمن السيبراني دون المساس بحقوق الخصوصية وحرية التعبير.
6. **تحديد الجرائم بدقة:** تعريف الجرائم الإلكترونية بشكل واضح ودقيق لتجنب التفسيرات الواسعة.

7. **تطوير آليات التعاون:** وضع إجراءات واضحة للتعاون بين الدول في التحقيقات وتبادل الأدلة الرقمية.
8. **التدريب المستمر:** تدريب المشرعين والقضاة على فهم التكنولوجيا والجرائم الإلكترونية.
9. **مشاركة أصحاب المصلحة:** إشراك القطاع الخاص والمجتمع المدني في عملية صياغة القوانين.
10. **المراجعة والتقييم:** تقييم فعالية القوانين بشكل دوري وتعديلها عند الضرورة.

هذه الخطوات تساعد في ضمان وجود إطار قانوني فعال وحديث لمواجهة التحديات المتطورة في مجال الجرائم الإلكترونية.

كيف يمكن توعية الجمهور عن مخاطر الجريمة الإلكترونية dangers of cybercrime

يمكن توعية الجمهور عن مخاطر الجرائم الإلكترونية من خلال عدة طرق فعالة:

1. **حملات توعية إعلامية:** استخدام وسائل الإعلام المختلفة لنشر معلومات عن أنواع الجرائم الإلكترونية وكيفية الحماية منها.
2. **برامج تعليمية في المدارس والجامعات:** إدراج مواد دراسية عن الأمن السيبراني والسلامة على الإنترنت.
3. **ورش عمل وندوات:** تنظيم فعاليات للجمهور وتعريفهم بالمخاطر وطرق الحماية.
4. **منشورات توعوية:** توزيع كتيبات ومنشورات تحتوي على نصائح وإرشادات حول الأمن الإلكتروني.
5. **استخدام وسائل التواصل الاجتماعي:** نشر معلومات وتحذيرات عبر المنصات الاجتماعية الشائعة.
6. **التعاون مع الشركات:** تشجيع الشركات على تدريب موظفيها وعملائها على الممارسات الآمنة عبر الإنترنت.
7. **إنشاء مواقع إلكترونية متخصصة:** توفير مصادر موثوقة للمعلومات حول الأمن السيبراني.
8. **تطبيقات الهواتف الذكية:** تطوير تطبيقات تقدم نصائح وتحذيرات حول الجرائم الإلكترونية.
9. **التعاون مع المؤثرين:** الاستعانة بالشخصيات المؤثرة لنشر الوعي بين متابعيهم.
10. **إقامة أيام وطنية للتوعية:** تخصيص أيام معينة للتركيز على قضايا الأمن السيبراني.
11. **توفير خطوط ساخنة:** إنشاء خطوط مساعدة لتقديم الدعم والمشورة للضحايا المحتملين.

12. **عرض دراسات حالة:** مشاركة قصص حقيقية عن ضحايا الجرائم الإلكترونية لزيادة الوعي بالمخاطر الواقعية.

هذه الاستراتيجيات المتنوعة تساعد في الوصول إلى شرائح مختلفة من المجتمع وزيادة الوعي العام بمخاطر الجرائم الإلكترونية.

الفصل الثاني

الجريمة الالكترونية والبنوك

الجرائم الإلكترونية تشكل تهديداً متزايداً للبنوك والمؤسسات المالية في العصر الرقمي. تتنوع هذه الجرائم لتشمل

القرصنة الإلكترونية واختراق أنظمة البنوك

الاستيلاء على بيانات البطاقات الائتمانية

الاحتيال والنصب الإلكتروني

سرقة الهويات والمعلومات الشخصية للعملاء

تواجه البنوك تحديات في مكافحة هذه الجرائم نظراً لتطورها المستمر وصعوبة تحديد تعريف موحد لها.

لذلك، تسعى الدول والمنظمات الدولية لتطوير أطر قانونية وتقنية لمواجهتها

لحماية نفسها وعملائها، تتخذ البنوك إجراءات مثل

-تعزيز أنظمة الأمن السيبراني

-تدريب الموظفين على التعرف على التهديدات

-تطوير آليات للكشف المبكر عن الاختراقات

-التعاون مع السلطات المختصة لمكافحة الجرائم الإلكترونية

يعد التكيف المستمر مع التطورات التكنولوجية والتعاون الدولي أمرين حاسمين في مكافحة الجرائم الإلكترونية في القطاع المصرفي

أبرز أنواع الجرائم الإلكترونية التي تؤثر على البنوك:

1. **القرصنة الإلكترونية:** اختراق أنظمة البنوك للوصول إلى البيانات الحساسة.
2. **سرقة بيانات البطاقات الائتمانية**: الاستيلاء على معلومات البطاقات لاستخدامها في عمليات غير مشروعة.
3. **الاحتيال الإلكتروني:** استخدام البريد الإلكتروني والإنترنت للاحتيال على العملاء والبنوك.
4. **تزوير الهوية:** سرقة المعلومات الشخصية واستخدامها لفتح حسابات أو إجراء معاملات غير قانونية.

5. **البرمجيات الخبيثة:** إصابة أنظمة البنوك بفيروسات وبرامج ضارة لسرقة البيانات أو تعطيل الخدمات.

الطرق التي يستخدمها المخترقون لارتكاب الجرائم الإلكترونية في البنوك

أبرز الطرق التي يستخدمها المخترقون لارتكاب الجرائم الإلكترونية في البنوك تشمل:

1. **القرصنة الإلكترونية**: اختراق أنظمة البنوك للوصول إلى البيانات الحساسة والمعلومات المالية للعملاء.
2. **انتحال الشخصية:** استخدام هويات مزورة أو مسروقة لفتح حسابات بنكية وهمية أو إجراء معاملات احتيالية.
3. **التصيد الاحتيالي**: إرسال رسائل إلكترونية مزيفة تبدو وكأنها من البنك لخداع العملاء وسرقة بياناتهم الشخصية والمالية.
4. **البرمجيات الخبيثة:** استخدام فيروسات وبرامج ضارة لاختراق أنظمة البنوك وسرقة المعلومات.
5. **الاحتيال عبر الإنترنت:** استخدام مواقع مزيفة تشبه مواقع البنوك الرسمية لسرقة بيانات تسجيل الدخول للعملاء.
6. **سرقة بيانات البطاقات الائتمانية:** استخدام تقنيات مختلفة لسرقة أرقام البطاقات وبياناتها لإجراء معاملات غير مصرح بها.
7. **الهندسة الاجتماعية:** استغلال العنصر البشري من خلال التلاعب النفسي للحصول على معلومات سرية من موظفي البنوك أو العملاء.

تقنيات الأمن السيبراني لمنع الجرائم الإلكترونية في البنوك

يمكن للبنوك استخدام تقنيات الأمن السيبراني لمنع الجرائم الإلكترونية من خلال:

1. تطبيق التشفير القوي لحماية البيانات المالية والمعلومات الحساسة للعملاء.
2. استخدام أنظمة متقدمة لاكتشاف التهديدات والاستجابة السريعة لأي محاولات اختراق.
3. تنفيذ خدمات الأمان السحابي لتشفير البيانات وتوفير آليات الوصول الآمن للمعلومات المالية في بيئات السحابة.
4. تطبيق أنظمة المصادقة متعددة العوامل للتحقق من هوية المستخدمين عند الدخول إلى الحسابات البنكية.

5. استخدام تقنيات الذكاء الاصطناعي وتحليل البيانات للكشف عن الأنماط المشبوهة والتصدي لها بسرعة.
6. تنفيذ أنظمة النسخ الاحتياطي والاحتياطات لضمان استمرارية الخدمات وتجنب فقد البيانات في حالة الهجمات.
7. تحديث مستمر لأنظمة الأمان وسد الثغرات الأمنية لمواكبة التهديدات المتطورة.
8. تدريب الموظفين على أحدث تقنيات الأمن السيبراني وكيفية التعامل مع التهديدات المحتملة.

هذه الإجراءات تساعد البنوك على تعزيز أمنها الإلكتروني وحماية أصولها ومعلومات عملائها من مخاطر الجرائم الإلكترونية المتزايدة.

الفصل الثالث

مكافحة الجريمة الإلكترونية

محاربة الجريمة الإلكترونية تحتاج لوقفة طويلة وقوية من قبل الدول والأفراد الكل مسؤول عن الإسهام قدر الإمكان محاربتها والتصدي لها.

تتجسد أول طرق مكافحة الجرائم الإلكترونية عبر الإنترنت في الاستدلال الذي يتضمن كل من التفتيش والمعاينة والخبرة والتي تعود إلى خصوصية الجريمة الإلكترونية عبر الإنترنت، أما الثاني سبل مكافحة الجريمة الإلكترونية هي تلك الجهود الدولية والداخلية لتجسيد قانونية للوقاية من هذه الجريمة المستحدثة، فأما الدولية فتتمثل في جهود الهيئات والمنظمات الدولية والتي تتمثل في:

1. توعية الناس لمفهوم الجريمة الإلكترونية وانه الخطر القائم ويجب مواجهته والحرص على ألا يقعوا ضحية له.
2. ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكي.
3. عدم الإفصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمات سر غير مألوفة.
4. عدم حفظ الصور الشخصية في الكمبيوتر.
5. عدم تنزيل أي ملف أو برنامج من مصادر غير معروفة.
6. الحرص على تحديث أنظمة الحماية مثل: استخدام برامج الحماية مثل نورتون norton، كاسبر سكي، مكافي.Mcafee...الخ.
7. تكوين منظمة لمكافحة الجريمة الإلكترونية.
8. ابلاغ الجهات المختصة في حال تعرض لجريمة إلكترونية.
9. تتبع تطورات الجريمة الإلكترونية وتطوير الرسائل والأجهزة والتشريعات لمكافحتها.

10. تطوير برمجيات امنة ونظم تشغيل قوية التي تحد من الاختراقات ذات التجسس وهي برامج تقوم بمسح الحاسب للبحث عن مكونات التجسس وإلغائها مثل: lavasoft

إثبات الجرائم الإلكترونية

إثبات الجرائم الإلكترونية يعتبر صعباً نظراً لطبيعتها المعقدة، ولكن هناك عدة طرق يمكن اتباعها:

اكتشاف الجريمة

- ملاحظة تلف البيانات أو تعديل الملفات الحساسة من قبل مدراء النظام.
- اكتشاف ولوج النظام باستخدام بيانات مستخدم مستحدثة.
- رصد أي نشاط غير معتاد على الشبكة أو الأنظمة.

التحقيق الجنائي الرقمي

- جمع وتحليل الأدلة الرقمية مثل سجلات الحاسوب وملفات التسجيل.
- الإطلاع على سجلات خلفية المنظمة وموظفيها.
- التعامل مع الحواسيب والشبكات ووسائط التخزين بطريقة آمنة لعدم طمس الأدلة.

الخبرة الفنية

- استشارة خبراء في تقنية المعلومات لديهم معرفة بالجرائم الإلكترونية.
- استخدام أدوات وبرامج متخصصة لاسترجاع البيانات المحذوفة أو المخفية.

عند اكتشاف جريمة إلكترونية، يجب اتخاذ الخطوات التالية بشكل فوري:

الحفاظ على الأدلة الرقمية

- عدم إغلاق الأجهزة أو الأنظمة المتضررة لتجنب فقدان أي بيانات أو أدلة رقمية.
- عزل الأجهزة المصابة عن الشبكة لمنع تلف المزيد من الأدلة.

- تجنب استخدام الأجهزة المصابة لأي غرض آخر حتى لا تطمس الأدلة.

الإبلاغ عن الجريمة

- الإبلاغ الفوري عن الجريمة للجهات الأمنية والقانونية المختصة.
- توفير أكبر قدر ممكن من المعلومات حول الجريمة والأضرار الناجمة عنها.
- الاحتفاظ بأي رسائل تهديد أو ابتزاز من الجناة إن وجدت.

التوثيق والتحقيق الأولي

- توثيق كل التفاصيل المتعلقة بالجريمة مثل التواريخ والأوقات والأشخاص المعنيين.
- البدء في التحقيق الأولي من خلال مراجعة سجلات النظام وملفات التسجيل.
- الاستعانة بخبراء في التحقيق الجنائي الرقمي إذا لزم الأمر.

اتباع هذه الخطوات الأولية بشكل صحيح يساعد على الحفاظ على الأدلة وتسهيل عملية التحقيق والملاحقة القانونية للجناة في وقت لاحق.

التعاون الدولي

- تفعيل اتفاقيات تسليم المجرمين الإلكترونيين بين الدول.
- التنسيق والتعاون بين أجهزة إنفاذ القانون الدولية لتتبع الجناة عبر الحدود.

بالرغم من الصعوبات، إلا أن اتباع هذه الخطوات بشكل احترافي يزيد من فرص إثبات الجرائم الإلكترونية وتقديم مرتكبيها للعدالة.

الجرائم الإلكترونية تعتبر خطيرة جداً وتشكل تهديداً كبيراً للأفراد والشركات والحكومات على حد سواء. وفيما يلي أبرز أسباب خطورتها:

- تتسم بالسرية وصعوبة الاكتشاف، حيث يمكن للمجرمين إخفاء هوياتهم وآثارهم بسهولة عبر الإنترنت.
- لا تعترف بالحدود الجغرافية، فهي جرائم عابرة للحدود يصعب التصدي لها.

- تستهدف أنظمة حساسة مثل البنوك والحكومات، مما يعرض البيانات الشخصية والمعلومات السرية للخطر.
- تتطلب مهارات متقدمة في تقنية المعلومات لارتكابها، مما يجعلها صعبة الإثبات.
- قد تكون لها دوافع سياسية أو إرهابية خطيرة مثل تدمير البنى التحتية أو اختراق الشبكات الحكومية.

لذلك، تعمل الدول على تشديد القوانين والتعاون الدولي لمكافحة هذه الجرائم ووضع إجراءات أمنية صارمة للحماية من الدافع المادي للحصول على مكاسب مالية.

الخطوات العملية الرئيسية لجمع الأدلة الجنائية الحاسوبية:

جمع الأدلة الجنائية الحاسوبية هو عملية دقيقة تتطلب اتباع خطوات منهجية لضمان سلامة الأدلة وقبولها في المحاكم. إليك الخطوات العملية الرئيسية لجمع الأدلة الجنائية الحاسوبية:

1. التحضير والتخطيط

- تحديد الأهداف: حدد الأهداف الرئيسية للتحقيق وما هي الأدلة التي تحتاج إلى جمعها.
- تشكيل فريق التحقيق: كوّن فريقًا من الخبراء في الأدلة الجنائية الحاسوبية، بما في ذلك المحققين والمحللين الفنيين.
- وضع خطة عمل: قم بوضع خطة عمل مفصلة تشمل جميع الخطوات التي سيتم اتخاذها لجمع الأدلة.

2. الحفاظ على مسرح الجريمة

- تأمين الموقع: تأكد من تأمين الموقع لمنع أي تدخل أو تلاعب بالأدلة.
- تسجيل كل شيء: قم بتوثيق كل شيء في مسرح الجريمة، بما في ذلك الأجهزة والمعدات الموجودة، باستخدام الصور والفيديو.

3. جمع الأدلة الأولية

- إيقاف تشغيل الأجهزة: إذا كان الجهاز قيد التشغيل، قم بإيقاف تشغيله بطريقة صحيحة لتجنب فقدان البيانات.
- فصل الأجهزة: افصل الأجهزة من الشبكة لمنع أي وصول غير مصرح به أو تلاعب بالبيانات.

4. تصوير الأدلة

- تصوير القرص الصلب: استخدم أدوات تصوير القرص الصلب لإنشاء نسخة طبق الأصل من البيانات الموجودة على القرص الصلب.
- تصوير الذاكرة: إذا كان الجهاز قيد التشغيل، قم بتصوير الذاكرة العشوائية (RAM) لجمع البيانات المؤقتة.

5. جمع البيانات الرقمية

- جمع البيانات من الأجهزة: اجمع البيانات من جميع الأجهزة ذات الصلة، بما في ذلك الحواسيب، الهواتف الذكية، والأجهزة اللوحية.
- جمع البيانات من الشبكة: اجمع سجلات الشبكة والبيانات المخزنة على الخوادم.

6. تحليل الأدلة

- تحليل البيانات: استخدم أدوات تحليل الأدلة الجنائية الحاسوبية لتحليل البيانات التي تم جمعها.
- البحث عن الأدلة: ابحث عن الأدلة التي تدعم التحقيق، مثل رسائل البريد الإلكتروني، سجلات الدردشة، والملفات المحذوفة.

7. توثيق الأدلة

- تسجيل العمليات: قم بتوثيق جميع العمليات التي تم تنفيذها لجمع الأدلة، بما في ذلك الأدوات المستخدمة والخطوات المتبعة.
- إعداد التقارير: قم بإعداد تقارير مفصلة توضح الأدلة التي تم جمعها وكيفية جمعها وتحليلها.

8. الحفاظ على سلسلة الحفظ

- تسجيل سلسلة الحفظ: تأكد من تسجيل سلسلة الحفظ لكل قطعة من الأدلة لضمان سلامتها وقبولها في المحكمة.
- تخزين الأدلة بأمان: قم بتخزين الأدلة في مكان آمن ومؤمن لمنع أي تلاعب أو فقدان.

9. التعاون مع الجهات القانونية

- التنسيق مع المحامين: تعاون مع المحامين والجهات القانونية لضمان أن الأدلة التي تم جمعها تتوافق مع المتطلبات القانونية.
- تقديم الأدلة في المحكمة: كن مستعدًا لتقديم الأدلة في المحكمة وتقديم الشهادات اللازمة لدعم التحقيق.

باتباع هذه الخطوات، يمكن للمحققين جمع الأدلة الجنائية الحاسوبية بطريقة منهجية وفعالة تضمن سلامة الأدلة وقبولها في الإجراءات القانونية.

الأدوات والبرامج المستخدمة في جمع الأدلة الجنائية الحاسوبية:

جمع الأدلة الجنائية الحاسوبية يتطلب استخدام مجموعة متنوعة من الأدوات والبرامج المتخصصة لضمان دقة وسلامة الأدلة. إليك بعض الأدوات والبرامج الرئيسية المستخدمة في هذا المجال.

1. أدوات تصوير القرص الصلب

- FTK Imager: أداة مجانية تتيح للمحققين إنشاء نسخ طبق الأصل من الأقراص الصلبة وتحليلها دون التأثير على البيانات الأصلية.
- EnCase: برنامج تجاري يستخدم على نطاق واسع في التحقيقات الجنائية الحاسوبية لتصوير وتحليل البيانات من الأقراص الصلبة.

2. أدوات تحليل البيانات

- Autopsy: أداة مفتوحة المصدر تحليل الأدلة الجنائية الحاسوبية، تتيح للمحققين فحص الملفات واستعادة البيانات المحذوفة.

- X-Ways Forensics: برنامج تجاري يوفر مجموعة واسعة من الأدوات لتحليل البيانات واستعادة الملفات المحذوفة.

3. أدوات تحليل الذاكرة

- Volatility: إطار عمل مفتوح المصدر لتحليل الذاكرة العشوائية (RAM)، يتيح للمحققين استخراج وتحليل البيانات من الذاكرة.
- Rekall: أداة أخرى مفتوحة المصدر لتحليل الذاكرة، تستخدم لإستخراج البيانات من الذاكرة العشوائية وتحليلها.

4. أدوات تحليل الشبكات

- Wireshark: أداة مفتوحة المصدر لتحليل حركة المرور على الشبكة، تتيح للمحققين فحص الحزم الشبكية واكتشاف الأنشطة المشبوهة.
- Networkminer: أداة لتحليل الشبكات تتيح استخراج البيانات من حركة المرور على الشبكة وتحليلها.

5. أدوات استعادة البيانات

- R-Studio: برنامج تجاري لاستعادة البيانات المحذوفة أو التالفة من الأقراص الصلبة والأجهزة الأخرى.
- PhotoRec: أداة مفتوحة المصدر لاستعادة الملفات المحذوفة من مجموعة متنوعة من الأجهزة.

6. أدوات إدارة الأدلة

- Case Management Software: برامج مثل Magnet AXIOM وunix توفر أدوات لإدارة الأدلة وتنظيمها وتوثيقها بشكل منهجي.

7. أدوات التحقق من الأصالة

- Hashing Tools: أدوات مثل MD5 SHA-1 تستخدم لإنشاء بصمات رقمية (hash values) للتحقق من سلامة البيانات وعدم تغييرها.

8. أدوات تحليل وسائل التواصل الاجتماعي

- Hunchly: أداة تساعد في جمع وتحليل الأدلة من مواقع التواصل الاجتماعي وتوثيقها.
- Social Media Examiner: برامج متخصصة في تحليل البيانات من منصات التواصل الاجتماعي وتقديم تقارير مفصلة.

9. أدوات تحليل الهواتف المحمولة

- Cellebrite UFED: أداة تجارية تستخدم لاستخراج وتحليل البيانات من الهواتف المحمولة.
- Oxygen Forensic Suite: برنامج تجاري آخر لتحليل البيانات من الأجهزة المحمولة.

10. أدوات التوثيق

- Snagit: أداة لتوثيق الأدلة عبر التقاط صور للشاشة وتسجيل الفيديو.
- Evernote: تطبيق لتدوين الملاحظات وتنظيمها، يمكن استخدامه لتوثيق خطوات جمع الأدلة.

استخدام هذه الأدوات والبرامج يساعد المحققين في جمع الأدلة الجنائية الحاسوبية بطريقة منهجية وفعالة، مما يضمن سلامة الأدلة وقبولها في الإجراءات القانونية.

كيف يمكن ضمان أمان الأدلة الجنائية الحاسوبية أثناء جمعها:

ضمان أمان الأدلة الجنائية الحاسوبية أثناء جمعها يتطلب اتباع مجموعة من الإجراءات والتقنيات لضمان سلامة الأدلة وقبولها في المحاكم. إليك بعض الخطوات الرئيسية لضمان أمان الأدلة الجنائية الحاسوبية:

1. تأمين مسرح الجريمة

- تأمين الموقع: تأكد من تأمين الموقع لمنع أي تدخل أو تلاعب بالأدلة.
- تسجيل كل شيء: قم بتوثيق كل شيء في مسرح الجريمة باستخدام الصور والفيديو لتسجيل حالة الأجهزة والمعدات.

2. استخدام أدوات موثوقة

- أدوات تصوير القرص الصلب: استخدم أدوات موثوقة مثل FTK Imager و EnCase لإنشاء نسخ طبق الأصل من الأقراص الصلبة.
- أدوات تحليل البيانات: استخدم برامج مثل Autopsy و X-Ways Forensics لتحليل البيانات دون التأثير على الأدلة الأصلية.

3. الحفاظ على سلسلة الحفظ

- تسجيل سلسلة الحفظ: تأكد من تسجيل سلسلة الحفظ لكل قطعة من الأدلة لضمان سلامتها وقبولها في المحكمة.
- تخزين الأدلة بأمان: قم بتخزين الأدلة في مكان آمن ومؤمن لمنع أي تلاعب أو فقدان.

4 . تشفير البيانات

- تشفير الأدلة: استخدم تقنيات التشفير لحماية البيانات الحساسة أثناء نقلها وتخزينها، مما يجعل من الصعب على المهاجمين الوصول إليها.

5. التوثيق الدقيق

- تسجيل العمليات: قم بتوثيق جميع العمليات التي تم تنفيذها لجمع الأدلة، بما في ذلك الأدوات المستخدمة والخطوات المتبعة.
- إعداد التقارير: قم بإعداد تقارير مفصلة توضح الأدلة التي تم جمعها وكيفية جمعها وتحليلها.

6. التدريب والتوعية

- التدريب المستمر: تقديم دورات تدريبية منتظمة للموظفين حول أفضل الممارسات في جمع الأدلة الجنائية الحاسوبية.
- التوعية بالأمن السيبراني: نشر الوعي بين الموظفين حول أهمية الأمن السيبراني وكيفية التعرف على التهديدات الإلكترونية.

7. استخدام تقنيات الحوسبة السحابية بأمان

- اختيار مزودي خدمات موثوقين: اختر مزودي خدمات الحوسبة السحابية الذين يقدمون مستويات عالية من الأمان والخصوصية.
- تطبيق سياسات الأمان: تأكد من تطبيق سياسات الأمان المناسبة عند استخدام خدمات الحوسبة السحابية لحماية البيانات من الاختراقات.

8. التعاون مع الجهات القانونية

- التنسيق مع المحامين: تعاون مع المحامين والجهات القانونية لضمان أن الأدلة التي تم جمعها تتوافق مع المتطلبات القانونية.
- تقديم الأدلة في المحكمة: كن مستعدًا لتقديم الأدلة في المحكمة وتقديم الشهادات اللازمة لدعم التحقيق.

باتباع هذه الخطوات، يمكن للمحققين ضمان أمان الأدلة الجنائية الحاسوبية أثناء جمعها، مما يضمن سلامة الأدلة وقبولها في الإجراءات القانونية.

كيف يمكن تأمين الأدلة الجنائية الحاسوبية أثناء النقل

يمكنني تقديم بعض الإرشادات العامة لتأمين هذه الأدلة استناداً إلى الممارسات المعتادة في مجال الأدلة الجنائية الرقمية:

1. **استخدام حاويات مؤمنة:** نقل الأدلة في حاويات مقاومة للصدمات ومضادة للكهرباء الساكنة ومختومة لمنع العبث.
2. **التشفير:** تشفير البيانات الرقمية أثناء النقل باستخدام خوارزميات تشفير قوية لحماية المحتوى من الوصول غير المصرح به.
3. **توثيق سلسلة الحفظ**: الاحتفاظ بسجل دقيق لكل من تعامل مع الأدلة، متى وأين، لضمان سلامتها القانونية.
4. **النسخ الاحتياطي**: إنشاء نسخ احتياطية متعددة من الأدلة قبل النقل وتخزينها بشكل آمن.
5. **النقل الآمن:** استخدام وسائل نقل موثوقة ومؤمنة، ويفضل أن يكون ذلك تحت إشراف مباشر من المحققين.
6. **تجنب الشبكات العامة**: عدم نقل الأدلة الرقمية عبر شبكات الإنترنت العامة غير المؤمنة.
7. **استخدام أجهزة تخزين آمنة:** نقل البيانات على أجهزة تخزين مشفرة و محمية بكلمات مرور قوية.
8. **التدريب المتخصص**: ضمان تدريب الأفراد المسؤولين عن نقل الأدلة على إجراءات الأمن والسلامة المناسبة.
9. **مراقبة الظروف البيئية**: التأكد من أن الأدلة محمية من الظروف البيئية القاسية مثل الحرارة الشديدة أو الرطوبة أثناء النقل.
10. **التوثيق الفوتوغرافي:** توثيق حالة الأدلة قبل وبعد النقل باستخدام الصور الفوتوغرافية.

هذه الإجراءات تساعد في الحفاظ على سلامة الأدلة الجنائية الحاسوبية وضمان قبولها في المحاكم.

التحديات التي تواجه استخدام الأدوات الجنائية الرقمية

تواجه استخدام الأدوات الجنائية الرقمية عدة تحديات رئيسية:

1. **التطور السريع للتكنولوجيا:** يتطلب تحديث مستمر للأدوات والمهارات لمواكبة التقنيات الجديدة والأساليب المتطورة للجرائم الإلكترونية.
2. **حجم البيانات الهائل:** مع زيادة سعة التخزين، يصبح فحص وتحليل كميات ضخمة من البيانات أكثر تعقيدًا وتستغرق وقتاً أطول.
3. **تشفير البيانات:** يمكن أن يعيق الوصول إلى الأدلة الرقمية ويتطلب تقنيات متقدمة لفك التشفير.
4. **الحفاظ على سلامة الأدلة:** يجب ضمان عدم تغيير البيانات الرقمية أثناء عملية التحليل للحفاظ على قبولها في المحكمة.
5. **التدريب المستمر:** يحتاج المحققون إلى تدريب مكثف ومستمر على الأدوات والتقنيات الجديدة.
6. **التعامل مع الأجهزة والبرمجيات المتنوعة:** تتطلب معرفة واسعة بمختلف الأنظمة والتطبيقات.
7. **الخصوصية والقضايا القانونية:** يجب موازنة الحاجة للأدلة مع حقوق الخصوصية وقوانين حماية البيانات.
8. **التعاون الدولي:** قد تتطلب الجرائم العابرة للحدود تنسيقًا بين الدول، مما يخلق تحديات قانونية ولوجستية.

التحديات التي تواجهها السلطات في مكافحة الجرائم الإلكترونية

تواجه السلطات القانونية والأمنية العديد من التحديات في مكافحة الجرائم الإلكترونية، ومنها:

التحديات القانونية

- صعوبة تطبيق القوانين التقليدية على الجرائم الإلكترونية بسبب طبيعتها المعقدة وعابرة للحدود الوطنية
- الحاجة إلى تحديث القوانين وإصدار تشريعات جديدة تتناسب مع التطورات التقنية السريعة
- تحدي إثبات الجرائم الإلكترونية وجمع الأدلة الرقمية بشكل قانوني.

التحديات التقنية

- التطور السريع للتقنيات المستخدمة في ارتكاب الجرائم الإلكترونية يتطلب متابعة مستمرة
- تنوع أساليب وتقنيات الجرائم الإلكترونية يصعب من تحديد الأساليب الفعالة لمكافحتها
- صعوبة الحصول على بيانات من مزودي الخدمة عن المتهمين مما يساعد على إخفاء الجريمة.

التحديات الدولية

- الحاجة إلى تعاون دولي لمكافحة الجرائم الإلكترونية العابرة للحدود
- اختلاف القوانين والتشريعات بين الدول يصعب من التعاون القانوني

لذلك، تحتاج السلطات إلى استراتيجيات متكاملة تجمع بين التشريعات القانونية المحدثة، والخبرات التقنية المتخصصة، والتعاون الدولي لمواجهة تحديات مكافحة الجرائم الإلكترونية بشكل فعال.

لمكافحة الجرائم الإلكترونية بشكل فعال، يجب اتباع استراتيجية متعددة الجوانب تجمع بين عدة عناصر رئيسية:

تحديث التشريعات القانونية

- إصدار قوانين وتشريعات حديثة تتناسب مع التطورات التقنية السريعة في مجال الجرائم الإلكترونية
- تسهيل عمليات التعاون القانوني والقضائي الدولي لملاحقة الجرائم عبر الحدود

تطوير القدرات التقنية

- تدريب فرق متخصصة في التحقيق في الجرائم الإلكترونية وجمع الأدلة الرقمية
- الاستثمار في تقنيات متطورة لرصد ومراقبة الأنشطة الإلكترونية المشبوهة
- التعاون مع شركات التقنية لتطوير حلول أمنية فعالة ضد التهديدات الإلكترونية

التوعية والتثقيف

- نشر الوعي لدى الأفراد والمؤسسات حول مخاطر الجرائم الإلكترونية وكيفية الحماية منها
- تضمين مناهج التوعية الأمنية الرقمية في المناهج التعليمية.

التعاون الدولي

- المشاركة في المنظمات والمبادرات الدولية لمكافحة الجرائم الإلكترونية
- تبادل المعلومات والخبرات مع الدول الأخرى لتعزيز الجهود المشتركة

من خلال الجمع بين هذه العناصر، يمكن للسلطات تطوير استراتيجية شاملة وفعالة لمواجهة التحديات المتنامية للجرائم الإلكترونية والحفاظ على الأمن الرقمي.

أهمية التوعية للحد من الجرائم الإلكترونية:

التوعية تلعب دوراً حيوياً في الحد من الجرائم الإلكترونية لعدة أسباب:

1. تساعد في تلافي المشاكل قبل وقوعها، مما يقلل من فرص نجاح الهجمات الإلكترونية.
2. تمكّن الأفراد من فهم خطورة هذه الجرائم واتخاذ الإجراءات الوقائية اللازمة.
3. تعزز الحذر من الروابط المشبوهة وعدم مشاركة المعلومات الشخصية عبر الإنترنت.
4. تشجع على حماية كلمات المرور وتغييرها بشكل مستمر، خاصة للحسابات المصرفية والائتمانية.
5. تنبه إلى أهمية عدم فتح رسائل إلكترونية من مصادر مجهولة لتجنب اختراق الأجهزة.
6. تساهم في حماية الحسابات المصرفية والمعلومات المالية والتجارية والبيانات الشخصية من الانتهاكات.
7. تعزز الفهم القانوني وتعرّف بمدى خطورة الجرائم الإلكترونية، مما يساعد في ردع المجرمين المحتملين.

من خلال هذه النقاط، يتضح أن التوعية تشكل خط الدفاع الأول ضد الجرائم الإلكترونية، وتمكّن الأفراد والمؤسسات من اتخاذ تدابير وقائية فعالة.

أفضل الطرق لتنفيذ برامج التوعية ضد الجرائم الإلكترونية

هناك عدة طرق فعالة لتنفيذ برامج التوعية ضد الجرائم الإلكترونية:

1. استخدام وسائل التواصل الاجتماعي لنشر معلومات توعوية بشكل منتظم حول أحدث التهديدات والممارسات الآمنة.
2. إقامة ورش عمل وندوات تفاعلية في المدارس والجامعات وأماكن العمل لتعليم الأفراد كيفية حماية أنفسهم.
3. إنتاج محتوى مرئي جذاب مثل مقاطع الفيديو القصيرة والرسوم المتحركة لتوضيح مخاطر الجرائم الإلكترونية بطريقة سهلة الفهم.
4. التعاون مع الشركات التقنية الكبرى لدمج رسائل التوعية في منتجاتها وخدماتها.
5. إطلاق حملات إعلانية على وسائل الإعلام التقليدية للوصول إلى شريحة أوسع من الجمهور.
6. تطوير تطبيقات وألعاب تعليمية تفاعلية لتعزيز الوعي بطريقة ممتعة.
7. تدريب المعلمين وقادة المجتمع ليكونوا سفراء للتوعية الأمنية في مجتمعاتهم.
8. إنشاء خط ساخن ومنصة إلكترونية لتقديم المشورة وتلقي البلاغات عن الحوادث الإلكترونية.
9. تنظيم مسابقات ومبادرات لتشجيع الشباب على المشاركة في نشر الوعي الأمني.
10. التعاون مع المؤثرين على وسائل التواصل الاجتماعي لنشر رسائل التوعية بين متابعيهم.

أفضل الممارسات لتحسين التوعية الأمنية الإلكترونية في المدارس:

لتحسين التوعية الأمنية الإلكترونية في المدارس، يمكن اتباع أفضل الممارسات التالية:

1. تصميم مناهج تعليمية مخصصة:
   - تطوير برامج تعليمية تناسب أعمار الطلاب لتعليمهم أساسيات الأمن السيبراني والممارسات الآمنة على الإنترنت.
2. تدريب المعلمين والإداريين:
   - تقديم دورات تدريبية للمعلمين والإداريين لتعريفهم بالمخاطر الإلكترونية وكيفية التعامل معها.
3. مشاركة أولياء الأمور:
   - تشجيع أولياء الأمور على المشاركة في تعزيز السلوكيات الآمنة على الإنترنت ومراقبة استخدام أبنائهم للتكنولوجيا.

4. حماية البيانات الشخصية:

- تطبيق أنظمة تشفير لحماية بيانات الطلاب الحساسة ومنع الوصول غير المصرح به.

5. استخدام تقنيات أمان متقدمة:

- استخدام برامج مكافحة الفيروسات وتطبيقات الأمان لحماية الأجهزة والشبكات المدرسية.

6. توعية الطلاب بالمخاطر الشائعة:

- تنظيم ورش عمل ومحاضرات توعوية حول مخاطر مثل التنمر الإلكتروني وسرقة الهوية وكيفية تجنبها.

7. تطوير سياسات أمان واضحة:

- وضع سياسات وإرشادات واضحة لاستخدام التكنولوجيا في المدرسة وضمان التزام الجميع بها.

هذه الممارسات تساعد في بناء بيئة تعليمية آمنة وتعزز الوعي الأمني لدى الطلاب والمعلمين.

أهم المبادرات الناجحة في تعزيز الأمن السيبراني لمكافحة الجريمة الالكترونية :

هناك العديد من المبادرات الناجحة التي تم تنفيذها لتعزيز الأمن السيبراني في مختلف الدول من بين هذه المبادرات:

- الإمارات العربية المتحدة

- مبادرة النبض السيبراني: تستهدف جميع شرائح المجتمع لنشر ثقافة الأمن السيبراني وتعزيز الوعي بأهمية حماية المعلومات الشخصية والبيانات الحساسة. هذه المبادرة هي جزء من جهود الإمارات لتبادل تجاربها الناجحة في مجال الأمن السيبراني مع العالم.

- مبادرة يوم الدفاع: أطلقها مجلس الأمن السيبراني في الإمارات، وتهدف إلى مشاركة المدارس في تعزيز ثقافة الأمن السيبراني بين الطلاب، مما يسهم في بناء جيل واعٍ ومؤهل لمواجهة التحديات السيبرانية.

- سلطنة عمان

-الجائزة الوطنية للأمن السيبراني: تتضمن ثلاث فئات رئيسية تركز على المبادرات ذات العائد الاقتصادي والاجتماعي، بما في ذلك التوعية في مجال الأمن السيبراني. تهدف هذه الجائزة إلى تعزيز مخرجات البرنامج الوطني لصناعة الأمن السيبراني.

- المملكة العربية السعودية

-أطلقت المملكة العربية السعودية مؤخراً ست مبادرات جديدة في مجال الأمن السيبراني خلال حدث معلوماتي بارز. تشمل هذه المبادرات تعزيز البنية التحتية للأمن السيبراني وتطوير القدرات الوطنية في هذا المجال.

- استراتيجيات عامة

- نهج قائم على المخاطر: تعتمد العديد من المنظمات استراتيجية قائمة على تحديد وتقييم مخاطر الأمن السيبراني وتحديد أولوياتها بناءً على تأثيرها المحتمل. هذا النهج يساعد في تخصيص الموارد بشكل فعال لتعزيز الأمن السيبراني.

وايضاً من المبادرات الناجحة في تعزيز الأمن السيبراني في المؤسسات التعليمية:

1. **مبادرة يوم الدفاع السيبراني**: أطلقها مجلس الأمن السيبراني لتعزيز وعي الطلاب والمدرسين بأهمية الأمن السيبراني من خلال فعاليات توعوية وتدريبية.
2. **برنامج "معًا" للأمن السيبراني**: أطلقه المركز الوطني للأمن السيبراني في البحرين، ويشمل مناهج تعليمية وأنشطة تفاعلية وألعاب إلكترونية لتعزيز مهارات الطلاب في الأمن السيبراني.
3. **المدرسة الافتراضية للأمن السيبراني**: في المملكة المتحدة، تهدف لتعليم المراهقين كيفية فك الرموز وإصلاح الثغرات الأمنية وتتبع الآثار الرقمية، من خلال ندوات إلكترونية يديرها خبراء.

هذه المبادرات والاستراتيجيات تعكس الجهود المستمرة لتعزيز الأمن السيبراني على مستوى الأفراد والمؤسسات والحكومات، مما يسهم في بناء بيئة رقمية أكثر أماناً وثقة.

في ختام الحديث عن الجرائم الإلكترونية، يمكن القول إن هذه الجرائم تشكل تهديداً كبيراً على مختلف جوانب الحياة، بما في ذلك الجوانب الاقتصادية والاجتماعية والنفسية. تتنوع الجرائم الإلكترونية من الاحتيال وسرقة الهوية إلى الابتزاز والتشهير، وتستهدف الأفراد والمؤسسات على حد سواء.

تتطلب مكافحة هذه الجرائم جهوداً متكاملة تشمل تعزيز الأمان الرقمي، وتحديث التشريعات، وتوعية المستخدمين بمخاطر الإنترنت. من الضروري أن يتخذ الأفراد والمؤسسات إجراءات وقائية مثل استخدام كلمات مرور قوية، وتحديث برامج الأمان، وتجنب الروابط المشبوهة، لضمان حماية المعلومات والبيانات من التهديدات الإلكترونية.

الاهداء

أهدي هذا الكتاب إلى:

1. الباحثين والمختصين في مجال الأمن السيبراني، الذين يكرسون جهودهم لفهم وتطوير سبل مكافحة الجرائم الإلكترونية.
2. رجال القانون والقضاء، الذين يواجهون تحديات جديدة في التعامل مع هذا النوع المستحدث من الجرائم.
3. ضحايا الجرائم الإلكترونية، الذين عانوا من آثارها المدمرة، على أمل أن يساهم هذا العمل في منع وقوع المزيد من الضحايا.
4. المبرمجين ومطوري البرمجيات، الذين يعملون على تطوير حلول أمنية لحماية المستخدمين.
5. المعلمين والمربين، الذين يقومون بدور حيوي في توعية الأجيال الجديدة بمخاطر العالم الرقمي.
6. كل مستخدم للإنترنت والتكنولوجيا الحديثة، على أمل أن يجد فيه ما يساعده على حماية نفسه وبياناته.
7. صناع القرار والمشرعين، الذين يسعون لوضع أطر قانونية فعالة لمواجهة هذه الظاهرة.

أخيراً، أهدي هذا العمل إلى كل من يؤمن بأهمية بناء عالم رقمي آمن وعادل للجميع.

الفهرس

أهم المصادر والمراجع

الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها	إعداد مركز البحوث والدراسات -بأكاديمية السلطان قابوس - عمان
موقع الأمم المتحدة	مكتب الأمم المتحدة المعني بالمخدرات والجريمة
International Cybercrime	ويكيبيديا -
Cybercrime Module 2 Key Issues	
Cybercrime _Cambridge University Press	
الجريدة الرسمية الليبية - القانون رقم 5 لسنة 2022	
قانون الجرائم الإلكترونية	ديوان التشريع والراي
قانون الجرائم الإلكترونية	موقع كاسبر سكاي
معاهدة الأمم المتحدة للجرائم الإلكترونية	معاهدة دولية لمكافحة الجرائم الإلكترونية منذ عام 2017

كتاب الجريمة الالكترونية كتاب قانوني - كل مايتعلق بالجرائم المعلوماتية والأمن السيبراني
كتابة وإعداد- أ٠ أريج عبد الرزاق بنيس
مراجعة وتدقيق - أ ٠م٠ مراد ترفاس
عدد صفحات الكتاب /84
تم تحريره في 10 أغسطس 2023
تم النشر في 15 أغسطس 2024

للتواصل مع الكاتب - البريد الالكتروني
arijbennis80@gmail.com